# Aplicación Citrix Workspace para Windows

# Contents



# Acerca de esta versión

April 6, 2023

## Novedades de la versión 2303

### Administración de aplicaciones cliente para el plug-in de WebEx [Technical Preview]

La descarga, la instalación y la actualización automática del plug-in de WebEx se admiten y se gestionan de la misma manera que los plug-ins de Zoom.

Para obtener más información sobre cómo habilitar esta función, consulte Administración de aplicaciones cliente para el plug-in de WebEx.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Puede enviar comentarios sobre esta función a través del formulario de Podio.

### Configurar la ruta para el almacenamiento de datos temporales del explorador web superpuesto de la redirección de contenido del explorador web

A partir de la versión 2303 de la aplicación Citrix Workspace, se le solicita que configure la ruta de almacenamiento de datos temporales para el explorador web basado en el Chromium Embedded Framework (CEF).

Para obtener más información, consulte Configurar la ruta para el almacenamiento de datos temporales del explorador web superpuesto de la redirección de contenido del explorador web.

### Compatibilidad con métodos de autenticación modernos para almacenes de StoreFront

La aplicación Citrix Workspace 2303 para Windows admite métodos de autenticación modernos para los almacenes de StoreFront. Puede autenticarse en los almacenes de Citrix StoreFront de cualquiera de las siguientes formas:

- Con claves de seguridad de Windows Hello y FIDO2. Para obtener más información, consulte Otras formas de autenticarse.

- Single Sign-On (SSO) en los almacenes de Citrix StoreFront desde máquinas unidas a Azure Active Directory (AAD) con AAD como proveedor de identidades. Para obtener más información, consulte Otras formas de autenticarse.
- Los administradores de Workspace pueden configurar y aplicar directivas de acceso condicional de Azure Active Directory para usuarios que se autentican en los almacenes de Citrix StoreFront. Para obtener más información, consulte Compatibilidad con el acceso condicional con Azure AD.

Para habilitar esta funcionalidad, debe utilizar Microsoft Edge WebView2 como explorador subyacente para la autenticación directa de StoreFront y la puerta de enlace.

> **Nota:**
>
> La versión de Microsoft Edge WebView2 Runtime debe ser 102 o posterior.

Puede habilitar métodos de autenticación modernos para los almacenes de StoreFront con la plantilla de objeto de directiva de grupo. Para obtener más información, consulte la sección Compatibilidad con métodos de autenticación modernos para almacenes de StoreFront.

#### Experiencia mejorada para llamadas de videoconferencia en Microsoft Teams optimizado

A partir de esta versión, la función de transmisión simultánea está habilitada de forma predeterminada para las llamadas de videoconferencia en Microsoft Teams optimizado. Con esta compatibilidad, la calidad y la experiencia de las videoconferencias en diferentes dispositivos de punto final mejoran al adaptarse a la resolución adecuada para ofrecer la mejor experiencia en llamadas a todos los usuarios.

Con esta experiencia mejorada, es posible que cada usuario cuente con varias transmisiones de vídeo en diferentes resoluciones (por ejemplo, 720p, 360p…) en función de varios factores, como la capacidad del dispositivo de punto final, las condiciones de la red y más. El dispositivo de punto final receptor solicita entonces la resolución de máxima calidad que pueda gestionar, lo que ofrece a todos los usuarios una experiencia de vídeo óptima.

> **Nota:**
>
> Esta función está disponible solamente después de la implantación de una actualización de Microsoft Teams. Para obtener información sobre ETA, vaya a y busque la hoja de ruta de Microsoft 365. Cuando Microsoft implante la actualización, consulte CTX253754 para obtener información sobre la actualización de la documentación y el anuncio.

#### Mejora de la protección de aplicaciones: Antiinyección de DLL

Como parte de la protección de aplicaciones, ahora contamos con una mejora de seguridad que ayuda a proteger la aplicación Citrix Workspace de determinadas bibliotecas de enlace dinámico (DLL) no

autorizadas o de módulos que no son de confianza. Si se inyectan estos módulos que no son de confianza, la aplicación Citrix Workspace detecta estas intervenciones e impide que los módulos se carguen.

La antiinyección de DLL se puede habilitar para estos componentes:

- Citrix Auth Manager
- Interfaz de usuario de la aplicación Citrix Workspace
- Citrix Virtual Apps and Desktops

Para obtener más información, consulte la documentación Protección de aplicaciones.

> **Aviso:**
>
> Esta característica funciona mediante el filtrado del acceso a las funciones necesarias del sistema operativo subyacente (llamadas a API específicas necesarias para cargar las DLL). De este modo, puede proporcionar protección incluso contra ciertas herramientas de piratas informáticos personalizadas y diseñadas específicamente. Sin embargo, a medida que los sistemas operativos evolucionan, pueden surgir nuevas formas de cargar archivos DLL. Si bien seguimos identificándolas y abordándolas, no podemos garantizar una protección completa en configuraciones e implementaciones específicas.

#### Citrix Enterprise Browser

Esta versión incluye la versión 109.1.1.29 de Citrix Enterprise Browser, basada en la versión 109 de Chromium. Para obtener más información sobre Citrix Enterprise Browser, consulte la documentación de Citrix Enterprise Browser.

#### Compatibilidad de Secure Private Access con StoreFront

Ahora, como administrador, puede configurar aplicaciones web y SaaS en StoreFront mediante una solución de Secure Private Access. Una vez que el administrador haya configurado la aplicación, los usuarios finales pueden abrir las aplicaciones web y SaaS mediante Citrix Enterprise Browser con una seguridad reforzada.

Para obtener más información, consulte Secure Private Access for on-premises en la documentación de Citrix Secure Private Access.

### Problemas resueltos en la versión 2303

- Las URL publicadas se abren a través de Citrix Enterprise Browser en lugar de abrirse con el explorador web predeterminado del dispositivo. [CTXBR-4718]
- Es posible que experimente demoras a la hora de enumerar aplicaciones e iniciar aplicaciones o escritorios cuando utilice SSON en un entorno que no tiene acceso activo a sitios externos. Este

problema se produce a partir de la versión 2210.5 de la aplicación Citrix Workspace y a partir de la versión 2203 CU2 de la aplicación Citrix Workspace. [CVADHELP-21786]

- Es posible que el proceso wfica32.exe se detenga de forma inesperada y aparezca un error al abrir una aplicación desde Citrix Workspace. Este problema solo se produce cuando la función de audio adaptable está habilitada. [CVADHELP-20999]
- Al instalar la aplicación Citrix Workspace 2212 en máquinas remotas mediante un script de PowerShell, es posible que el instalador de la aplicación Citrix Workspace se detenga. Este problema se produce antes de que comience la instalación en la máquina remota. [CVADHELP-22278]
- Al intentar configurar varios almacenes mediante un objeto de directiva de grupo (GPO) o una línea de comandos, es posible que uno de los almacenes no esté completamente configurado. [CVADHELP-22034]
- Es posible que la pantalla muestre la ventana emergente de autenticación en la esquina superior izquierda en lugar de mostrarse en el centro. [CVADHELP-21835]
- Una vez que se haya agregado un almacén con el token de autenticación del almacén establecido en **true**, es posible que Citrix Workspace deje de responder en la pantalla blanca y que el token de autenticación del almacén pase a estar en **false**. [CVADHELP-21582]
- Es posible que no pueda acceder a la aplicación Citrix Workspace para Windows cuando la VPN se desconecta o se conecta de nuevo. [CVADHELP-21662]
- Al compartir una pantalla con Microsoft Teams desde los dispositivos de punto final HP EliteBook G6, es posible que vea una ventana roja en lugar de un borde rojo. [CVADHELP-20763]
- Es posible que no pueda utilizar la aplicación Bloomberg Terminal con el teclado Bloomberg 5 o el teclado Bloomberg 2013. Este problema se produce cuando la versión 2302 de la aplicación Citrix Workspace está instalada en el sistema con la función de protección de aplicaciones habilitada. [CVADHELP-22221]
- Es posible que la posición y el tamaño de la ventana no se conserven al reconectar el escritorio. Este problema se produce cuando el escritorio está en el modo Ventana y utiliza un monitor que no es el principal. [HDX-44997]
- La barra de herramientas de **Desktop Viewer** podría cubrir la pantalla cuando el escritorio tiene una resolución y PPP normales. [HDX-45206]
- En un caso con varias sesiones, al abrir una segunda sesión, es posible que la sesión quedé oculta detrás de la primera sesión. Además, es posible que el icono de la aplicación Citrix Workspace de la segunda sesión no esté presente en la barra de tareas. [RFWIN-29773]

### Problemas conocidos en la versión 2303

- Es posible que la aplicación Citrix Workspace deje de responder si interactúa con el mouse (una acción o un movimiento del mouse) en el cuadro de diálogo **Restaurar sesión**. Este problema se produce al iniciar una sesión después de actualizar la aplicación Citrix Workspace de la versión 2302 a la versión 2303 y si había sesiones desconectadas. [RFWIN-29663]

> **Nota:**
>
> Para obtener una lista completa de los problemas de las versiones anteriores, consulte Problemas conocidos.

### Versiones anteriores

En esta sección se proporciona información sobre las nuevas funciones y los problemas resueltos en las versiones anteriores disponibles según lo indicado en Lifecycle Milestones for Citrix Workspace app.

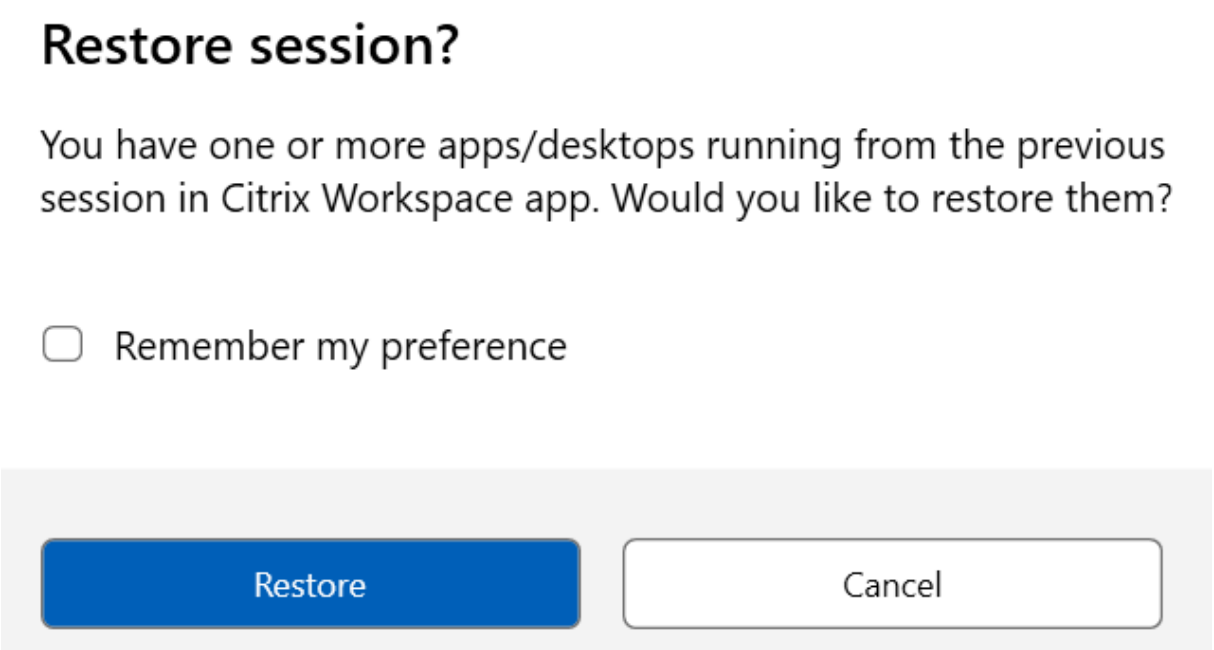
#### 2302

##### Novedades

**Experiencia mejorada al reconectar aplicaciones y escritorios virtuales**

Esta versión ofrece una experiencia de usuario mejorada al reconectarse a aplicaciones y escritorios virtuales de los que se había desconectado.

Cuando la aplicación Citrix Workspace intenta actualizar la aplicación Citrix Workspace desconectada o iniciar nuevas aplicaciones o escritorios virtuales como parte de la funcionalidad de control del espacio de trabajo, aparece el siguiente mensaje:




Este mensaje solo aparece cuando la opción para **mostrar la solicitud de reconexión para volver a conectar las sesiones** se establece en “true” en Global App Configuration Service.

Haga clic en **Restaurar** para volver a conectarse y abrir las aplicaciones y escritorios virtuales nuevos y desconectados. Si solo quiere iniciar las aplicaciones y escritorios recién seleccionados, haga clic en **Cancelar**.

También puede seleccionar la opción **Recordar mi preferencia** para aplicar la preferencia seleccionada al siguiente inicio de sesión.

El mensaje **¿Restaurar sesión?** anterior aparecerá solo si:

- el usuario intenta iniciar una aplicación perteneciente a un almacén del espacio de trabajo;
- las directivas administrativas o los parámetros de configuración de la aplicación no están configurados para la funcionalidad de control del espacio de trabajo;
- las opciones de reconexión de control del espacio de trabajo están configuradas de forma predeterminada en el cliente.

> **Nota:**
>
> La configuración de reconexión de **Opciones de reconexión** tiene prioridad sobre las preferencias establecidas en el cuadro de diálogo. Para obtener más información, consulte Configurar opciones de reconexión mediante el cuadro de diálogo Preferencias avanzadas.

#### Administración de aplicaciones cliente para el plug-in de Zoom

Ahora puede administrar el plug-in de Zoom mediante la función Administración de aplicaciones cliente.

> **Nota:**
>
> Esta funcionalidad solo es aplicable a las sesiones de Workspace (en la nube).

Para obtener más información, consulte Administración de aplicaciones cliente para el plug-in de Zoom.

#### Compatibilidad con métodos de autenticación modernos para almacenes de StoreFront [Technical Preview]

A partir de esta versión, la aplicación Citrix Workspace para Windows admite métodos de autenticación modernos para los almacenes de StoreFront. Puede autenticarse en los almacenes de Citrix StoreFront de cualquiera de las siguientes formas:

- Con claves de seguridad de Windows Hello y FIDO2. Para obtener más información, consulte Otras formas de autenticarse.
- Single Sign-On (SSO) en los almacenes de Citrix StoreFront desde máquinas unidas a Azure Active Directory (AAD) con AAD como proveedor de identidades. Para obtener más información, consulte Otras formas de autenticarse.

- Los administradores de Workspace pueden configurar y aplicar directivas de acceso condicional de Azure Active Directory para usuarios que se autentican en los almacenes de Citrix StoreFront. Para obtener más información, consulte Compatibilidad con el acceso condicional con Azure AD.

Para habilitar esta funcionalidad, debe utilizar Microsoft Edge WebView2 como explorador subyacente para la autenticación directa de StoreFront y la puerta de enlace.

> **Nota:**
>
> La versión de Microsoft Edge WebView2 Runtime debe ser 102 o posterior.

Puede habilitar métodos de autenticación modernos para los almacenes de StoreFront con la plantilla de objeto de directiva de grupo. Para obtener más información, consulte la sección Compatibilidad con métodos de autenticación modernos para almacenes de StoreFront.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Puede enviar comentarios sobre esta función a través del formulario de Podio.

### Se ha actualizado el modo de selección de dispositivos de audio para Microsoft Teams optimizado

A partir de esta versión, al cambiar los dispositivos de audio predeterminados en la configuración de sonido del dispositivo de punto final, Microsoft Teams optimizado en la imagen de disco virtual (VDI) de Citrix VDI cambia la selección actual de dispositivos de audio para que coincida con los valores predeterminados del dispositivo de punto final.

Sin embargo, si selecciona un dispositivo de forma explícita en Microsoft Teams, su selección tendrá prioridad y no seguirá los valores predeterminados del dispositivo de punto final. Su selección se mantendrá hasta que borre la memoria caché de Microsoft Teams.

### Mejora en la protección de aplicaciones

A partir de esta versión, la aplicación Citrix Workspace para Windows permite configurar la protección de aplicaciones para la autenticación y para Self-Service plug-in mediante Global App Configuration Service. Anteriormente, solo se podían configurar estos componentes mediante el objeto de directiva de grupo.

Si habilita las funciones de protección contra registro de tecleo y contra la captura de pantalla mediante Global App Configuration Service, se aplicarán tanto a la autenticación como a Self-service Plug-in.

> **Nota:**
>
> Las configuraciones de Global App Configuration Service no afectan a las aplicaciones virtuales, los escritorios virtuales, las aplicaciones web y las aplicaciones SaaS. Estos recursos se siguen controlando mediante el Delivery Controller y Citrix Secure Private Access. Para obtener más información, consulte la sección de configuración de Protección de aplicaciones en la documentación de Citrix Virtual Apps and Desktops.

Para obtener más información, consulte la sección Mejora en la protección de aplicaciones.

### Citrix Enterprise Browser

Esta versión incluye la versión 108.1.1.97 de Citrix Enterprise Browser, basada en la versión 108 de Chromium. Para obtener más información sobre Citrix Enterprise Browser, consulte la documentación de Citrix Enterprise Browser.

### Abrir todas las aplicaciones web y SaaS a través de Citrix Enterprise Browser

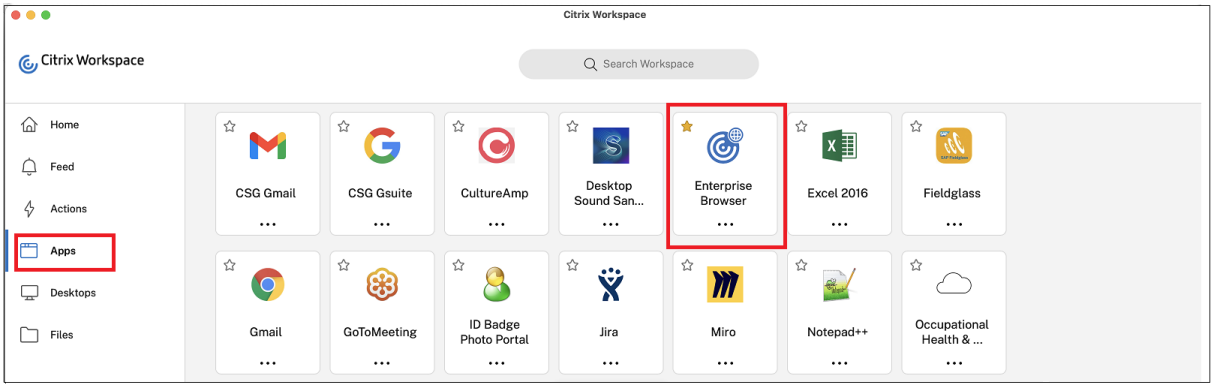
En esta versión de Enterprise Browser (en la aplicación Citrix Workspace para Windows), todas las aplicaciones web internas y las aplicaciones SaaS externas disponibles en la aplicación Citrix Workspace se abren en Citrix Enterprise Browser.

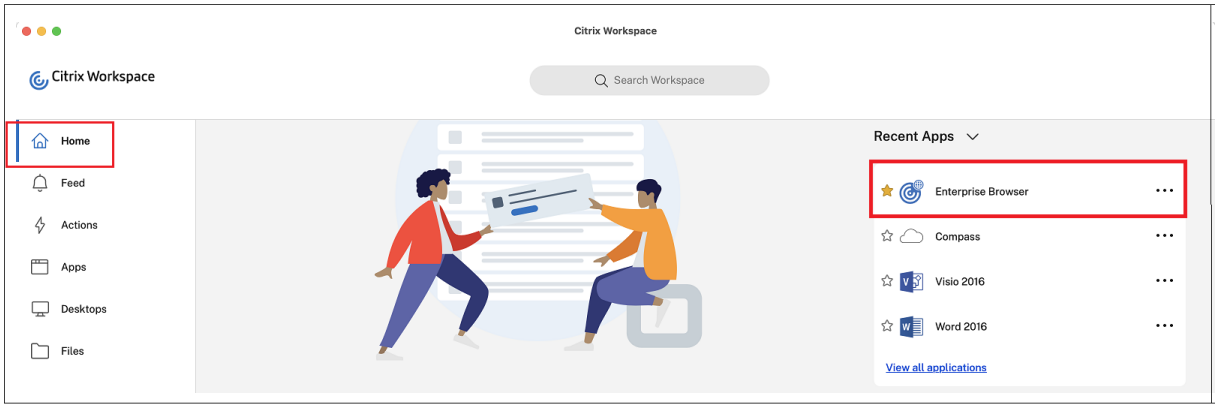
### Opción para iniciar Citrix Enterprise Browser desde la aplicación Citrix Workspace

Anteriormente, Citrix Enterprise Browser solo se podía abrir desde la aplicación Citrix Workspace después de abrir una aplicación web o SaaS.

A partir de esta versión, Enterprise Browser se puede abrir directamente desde la aplicación Citrix Workspace sin necesidad de abrir una aplicación web o SaaS. Esta función proporciona un acceso sencillo a Citrix Enterprise Browser y no requiere ninguna configuración por parte de los administradores. Esta función está disponible de forma predeterminada.




> **Nota:**
>
> El usuario final debe tener asignados derechos con relación a, al menos, una aplicación web o SaaS a través de Secure Private Access.

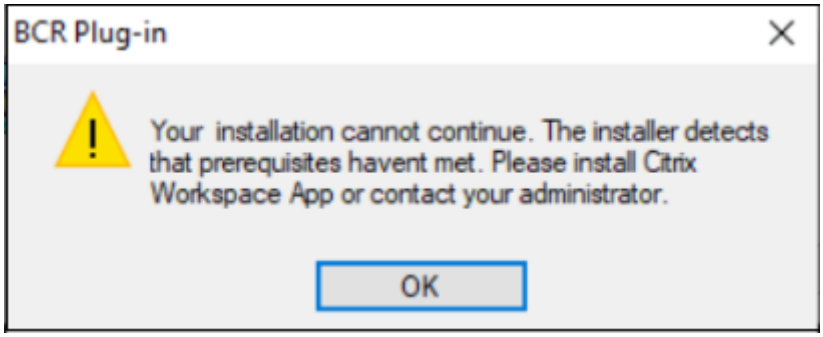
### Problemas resueltos

- Algunas aplicaciones SaaS que tienen la seguridad mejorada **desactivada** no se abren en Citrix Enterprise Browser cuando este es el explorador predeterminado. [CTXBR-4106] [CTXBR-4405]
- Los intentos de iniciar aplicaciones o escritorios desde almacenes web personalizados pueden fallar cuando se utiliza Microsoft Edge WebView2 Runtime 109 y versiones posteriores. [RFWIN-29200].
- Es posible que no pueda agregar un almacén oculto a la aplicación Citrix Workspace. Este problema ocurre cuando se intenta agregar un nombre de dominio completo (FQDN) de Citrix Gateway que requiere autenticación con tarjeta inteligente o cuando el nombre del almacén de StoreFront contiene espacios, por ejemplo, `https://servername.company.com?Store` Service. [CVADHELP-21516]
- Es posible que el valor de tiempo de espera por inactividad no caduque si sale de la aplicación Citrix Workspace antes de alcanzar el valor de tiempo de espera establecido. Como resultado, es

posible que más adelante pueda iniciar la aplicación Citrix Workspace sin necesidad introducir ninguna credencial. [CVADHELP-20912]

- Puede que no se vea automáticamente la página emergente de autenticación después de instalar la aplicación Citrix Workspace. [CVADHELP-20593]
- En una configuración con varios monitores, las ventanas de las aplicaciones se mueven a un monitor diferente cada vez que el usuario se desconecta y se vuelve a conectar a la sesión. [HDX-45043]
- En algunas series antiguas de la GPU AMD, es posible que aparezca contenido de vídeo morado o pantallas parpadeantes con la aplicación Citrix Workspace 2206 o una versión posterior. [HDX-46264]
- No se puede reparar el archivo BCRClient.msi y aparece el siguiente error durante la instalación de la aplicación Citrix Workspace:




[HDX-46964]

## 2212

### Novedades

> **Nota:**
>
> A partir de esta versión, asegúrese de que la versión de Microsoft Edge WebView2 Runtime sea 102 o una posterior. Para obtener más información, consulte Requisitos del sistema y compatibilidad.

#### Administración de aplicaciones cliente

La aplicación Citrix Workspace 2212 para Windows ahora ofrece funcionalidad de administración de aplicaciones cliente, lo que la convierte en la única aplicación cliente necesaria en el dispositivo de punto final para instalar y administrar agentes, como el agente de Secure Access y el plug-in End Point Analysis (EPA).

Con esta capacidad, los administradores pueden implementar y administrar fácilmente los agentes necesarios desde una única consola de administración.

> **Nota:**
>
> Esta funcionalidad solo es aplicable a las sesiones de Workspace (en la nube).

Para obtener más información, consulte Administración de aplicaciones cliente.

#### Administración de aplicaciones cliente para el plug-in de Zoom [Technical Preview]

A partir de la aplicación Citrix Workspace 2212 para Windows, puede administrar el plug-in de Zoom mediante la funcionalidad de administración de aplicaciones cliente.

> **Nota:**
>
> Esta funcionalidad solo es aplicable a las sesiones de Workspace (en la nube).

Para obtener más información, consulte Administración de aplicaciones cliente.

Puede registrar sus comentarios sobre esta Technical Preview en este formulario de Podio.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

#### Control de versiones con actualización automática

Ahora, los administradores pueden administrar la versión de las actualizaciones automáticas de los dispositivos de la organización.

Los administradores pueden controlar la versión estableciéndola en la propiedad maximumAllowed-Version de Global App Config Service.

Ejemplo de archivo JSON en Global App Config Service:

```
"AutoUpdate": {


"userOverride": false,

"AutoUpdatePluginsSettings": [

    {

```

```
10
11      "pluginSettings":
12
13  {
14          "upgradeToLatest": false,
15          "maximumAllowedVersion": "22.9.0.3934",                  }
16
17
18  ,
19
20      "pluginName": "WorkspaceApp",
21
22      "pluginId": "1CDF566D-B2C7-47F-6283C862E1D6"
23
24     }
25
26
27  <!--NeedCopy-->
```

Cuando se establece la versión, la aplicación Citrix Workspace del dispositivo del usuario se actualiza automáticamente con la versión especificada en la propiedad maximumAllowedVersion.

> **Notas:**
>
> - Para efectuar el control de versiones de las actualizaciones automáticas, el parámetro `upgradeToLatest` de Global App Config Service debe estar establecido en false. Si tiene el valor true, `maximumAllowedVersion` se ignora.
> - No modifique pluginId, ya que es el ID asignado a la aplicación Citrix Workspace.
> - Si el administrador no ha configurado la versión en Global App Config Service, la aplicación Citrix Workspace se actualiza a la versión disponible más reciente de forma predeterminada.

#### Forzar solicitud de inicio de sesión para el proveedor de identidades federadas

La aplicación Citrix Workspace ahora respeta la configuración sobre sesiones de proveedores de identidades federadas. Para obtener más información, consulte el artículo CTX253779 de Citrix Knowledge Center.

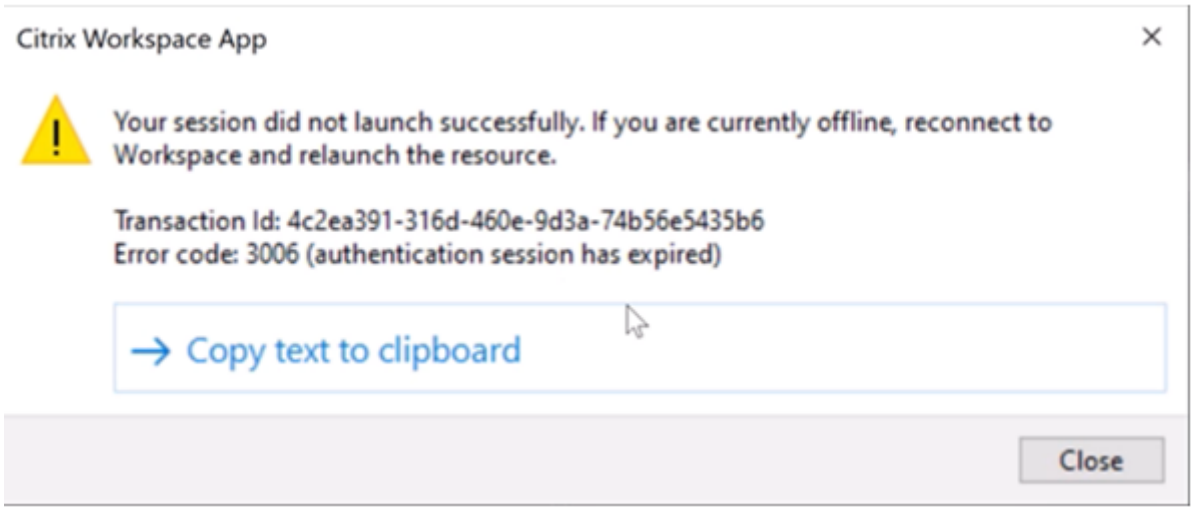
Ya no es necesario usar la directiva Almacenar tokens de autenticación para forzar la solicitud de inicio de sesión.

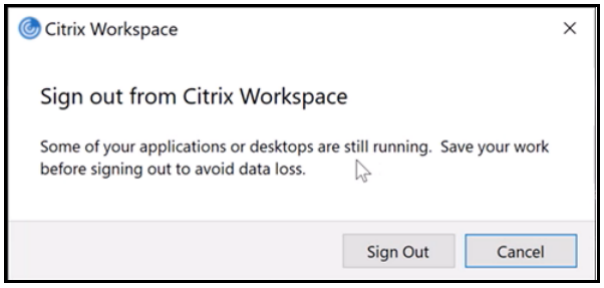
#### Mejora de la experiencia de reconexión tras la caducidad del archivo de concesión de conexiones

Anteriormente, el usuario final no recibía ninguna notificación cuando el archivo de concesión de conexiones y el token de autenticación caducaban.

A partir de esta versión, aparece un mensaje de error y un cuadro de diálogo de consentimiento. El cuadro de diálogo de consentimiento solo aparece cuando hay recursos ejecutándose en la sesión. Si no hay recursos en ejecución, solo aparece el cuadro de diálogo de error. Se cierra la sesión sin que aparezca el cuadro de diálogo de consentimiento.




Puede hacer clic en **Cerrar sesión** para cerrar la sesión actual de la aplicación Citrix Workspace o en **Cancelar** para continuar con la sesión.

> **Nota:**
>
> Guarde sus datos antes de hacer clic en **Cerrar sesión**.

#### Mejora de la protección de aplicaciones: Antiinyección de DLL [Technical Preview]

Como parte de la protección de aplicaciones, ahora contamos con una mejora de seguridad que ayuda a proteger la aplicación Citrix Workspace de determinadas bibliotecas de enlace dinámico (DLL) no autorizadas o de módulos que no son de confianza. Si se inyectan estos módulos que no son de confianza, la aplicación Citrix Workspace detecta estas intervenciones e impide que los módulos se carguen.

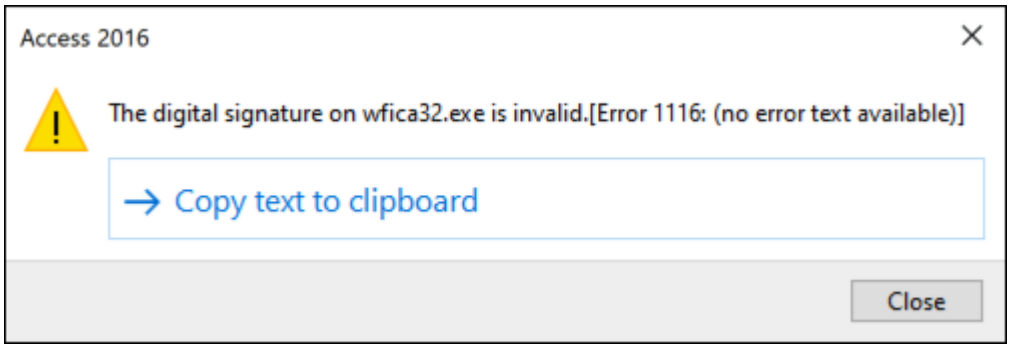
 

Anteriormente, esta funcionalidad de Technical Preview solo se aplicaba a aplicaciones y escritorios virtuales protegidos. Con esta versión, hemos ampliado su alcance para incluir ahora:

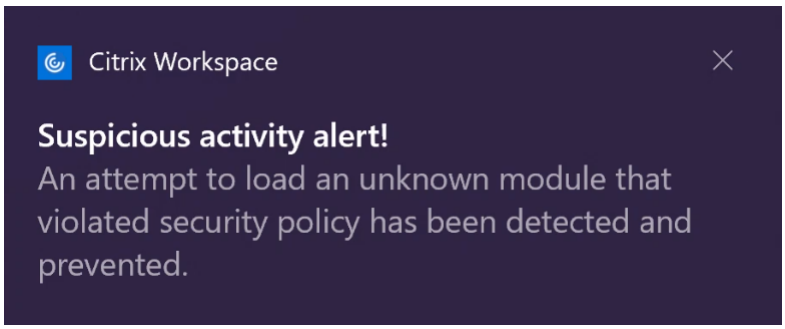
- Todas las sesiones de aplicaciones y escritorios virtuales
- La ventana de autenticación de la aplicación Citrix Workspace (implementación local o StoreFront)

Además, esta mejora ahora:

- cierra la sesión inmediatamente cuando existen determinadas DLL maliciosas o que no son de confianza en el componente protegido




- Muestra una notificación cuando se bloquea una DLL maliciosa o que no es de confianza.




**Renuncia de responsabilidades:**

Esta característica funciona filtrando el acceso a las funciones necesarias del sistema operativo subyacente (llamadas a API específicas necesarias para cargar las DLL). De este modo, puede proporcionar protección incluso contra ciertas herramientas de piratas informáticos personalizadas y diseñadas específicamente.  Sin embargo, a medida que los sistemas operativos evolucionan, pueden surgir nuevas formas de cargar archivos DLL. Si bien seguimos identificándolas y abordándolas, no podemos garantizar una protección completa en configuraciones e implementaciones específicas.

Puede registrarse para obtener esta versión Technical Preview a través de este formulario de Podio.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de

> compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

**Compatibilidad con la instalación predeterminada de Protección de aplicaciones**

El componente Protección de aplicaciones ahora se instala de forma predeterminada durante la instalación de la aplicación Citrix Workspace.

La casilla Habilitar protección de aplicaciones que aparece durante la instalación se sustituye por Iniciar protección de aplicaciones tras la instalación.


Al seleccionar esta casilla de verificación, Protección de aplicaciones se inicia inmediatamente después de la instalación.

> **Nota:**
>
> Si no se habilita esta casilla de verificación, Protección de aplicaciones se inicia automáticamente al iniciar por primera vez un recurso o componente protegido en el caso de los clientes que tienen asignado el derecho de uso del componente Protección de aplicaciones.

También puede iniciar el componente Protección de aplicaciones mediante el parámetro `/startappprotection` de línea de comandos. Sin embargo, el conmutador `/includeappprotection`

anterior se ha retirado.

> **Nota:**
>
> Anteriormente, las funcionalidades de protección contra la captura de tecleo y contra las capturas de pantalla se aplicaban de forma predeterminada para la autenticación de Citrix y las pantallas de la aplicación Citrix Workspace. Sin embargo, a partir de 2212, estas capacidades están inhabilitadas de forma predeterminada y deben configurarse mediante el objeto de directiva de grupo. Para obtener información sobre la configuración del objeto de directiva de grupo, consulte Mejora de la configuración de protección de aplicaciones.

#### Mejora de la protección de aplicaciones: Detección y notificación de capturas de pantalla

A partir de esta versión, podrá ver una notificación cuando haya un posible intento de captura de pantalla con relación a cualquier recurso protegido. Para obtener información sobre los recursos protegidos con Protección de aplicaciones, consulte ¿Qué protege la protección de aplicaciones?

La notificación aparece cuando hay:

- Un intento de hacer una captura de pantalla o grabar un vídeo a través de una herramienta para captura de pantallas.
- Un intento de hacer una captura de pantalla con la tecla Imprimir pantalla.

> **Nota:**
>
> La notificación aparece solo una vez por instancia en ejecución de la herramienta de captura de pantallas. La notificación vuelve a aparecer si reinicia la herramienta e intenta capturar una pantalla.

#### Optimización de Desktop Viewer

Esta versión optimiza la experiencia con Desktop Viewer al reducir el tiempo de inicio en 5 segundos. La barra de herramientas de Desktop Viewer se abre rápidamente y puede mostrar la pantalla de inicio de sesión predeterminada de Windows. Los administradores pueden ocultarla configurando la siguiente clave de Registro para introducir cierto retraso en milisegundos:

- Ubicación: HKEY_CURRENT_USER\SOFTWARE\Citrix\XenDesktop\DesktopViewer
- Nombre: ExtendConnectScreenMS
- Tipo: DWORD
- Valor: 00000000 (retraso en milisegundos)

> **Nota:**
>
> La configuración del Registro es opcional.

### Citrix Enterprise Browser

> **Nota:**
>
> A partir de la versión 2210 de la aplicación Citrix Workspace para Windows, la función **Abrir todas las aplicaciones web y SaaS a través de Citrix Enterprise Browser** está inhabilitada.

Esta versión incluye la versión 107.1.1.13 de Citrix Enterprise Browser, basada en la versión 107 de Chromium. Para obtener más información sobre Citrix Enterprise Browser, consulte la documentación de Citrix Enterprise Browser.

- **Configurar Citrix Enterprise Browser como explorador de trabajo**

  Ahora puede configurar Citrix Enterprise Browser como explorador de trabajo para abrir todos los enlaces de trabajo. Puede seleccionar un explorador alternativo para abrir los enlaces que no sean de trabajo.

  Un enlace de trabajo es un enlace asociado a las aplicaciones web o SaaS configuradas por el administrador para el usuario final. Cuando un usuario hace clic en cualquier enlace de una aplicación nativa, si se trata de un enlace de trabajo, se abre a través de Citrix Enterprise Browser. De lo contrario, se abre a través del explorador alternativo que seleccione el usuario final.

  Para obtener más información, consulte Configurar Citrix Enterprise Browser como explorador de trabajo.

### Problemas resueltos en la versión 2212

- La aplicación Citrix Workspace le pide que seleccione un certificado aunque solo exista un certificado. Este problema se produce al autenticarse en el almacén (de la nube) de Workspace. Para suprimir esta solicitud de certificado, agregue este Registro:

  On 32-bit systems:

  - Location: HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle or HKEY_CURRENT_USER\Software\Citrix\Da
  - Name: SuppressCertSelectionPrompt
  - Type: String
  - Value: True

  On 64-bit systems

  - Location: HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle or HKEY_CURRENT_USER\So
  - Name: SuppressCertSelectionPrompt
  - Type: String
  - Value: True

  [CVADHELP-20844]

- Es posible que no pueda acceder a la aplicación Citrix Workspace para Windows cuando la VPN se desconecta o se conecta de nuevo [CVADHELP-20376]
- No se pudo detectar End Point Analysis (EPA) durante la autenticación en el almacén configurado con EPA. Este problema se produce al actualizar la aplicación Citrix Workspace de la versión anterior a la 2210 o posterior. [CVADHELP-21387]
- Durante una llamada optimizada de Microsoft Teams, es posible que el dispositivo de punto final entre en el estado de suspensión. [HDX-44438]
- Citrix Analytics no puede recibir métricas relacionadas con la red de los usuarios finales. Este problema se produce incluso cuando se cumplen estos requisitos previos:
  - Las sesiones de aplicación o escritorio permanecen en ejecución durante más de 15 minutos con la aplicación Citrix Workspace.
  - El almacén o la cuenta utilizados están habilitados para CAS.

  > **Nota:**
  >
  > Los eventos de CAS relacionados con la red no se envían para el inicio de aplicaciones o escritorios basado en explorador. Se envían solo cuando se abre la aplicación o el escritorio a través de la web y desde el mismo almacén que se agrega a través de la aplicación Citrix Workspace nativa.

  [CVADHELP-21448]
- Al abrir una aplicación publicada en modo integrado, es posible que otras aplicaciones locales o integradas aparezcan en primer plano y tapen la aplicación publicada. [CVADHELP-20742]

## 2210.5

### Novedades

En esta versión se han resuelto problemas para mejorar la estabilidad, la seguridad y el rendimiento general.

### Administración de aplicaciones cliente [Technical Preview]

La aplicación Citrix Workspace 2210.5 para Windows ahora ofrece funcionalidad de administración de aplicaciones cliente, lo que la convierte en la única aplicación cliente necesaria en el dispositivo de punto final para instalar y administrar agentes, como el agente de Secure Access y el plug-in de End Point Analysis (EPA).

Con esta capacidad, los administradores pueden implementar y administrar fácilmente los agentes necesarios desde una única consola de administración.

**Nota:** Esta funcionalidad solo es aplicable a las sesiones de Workspace (en la nube).

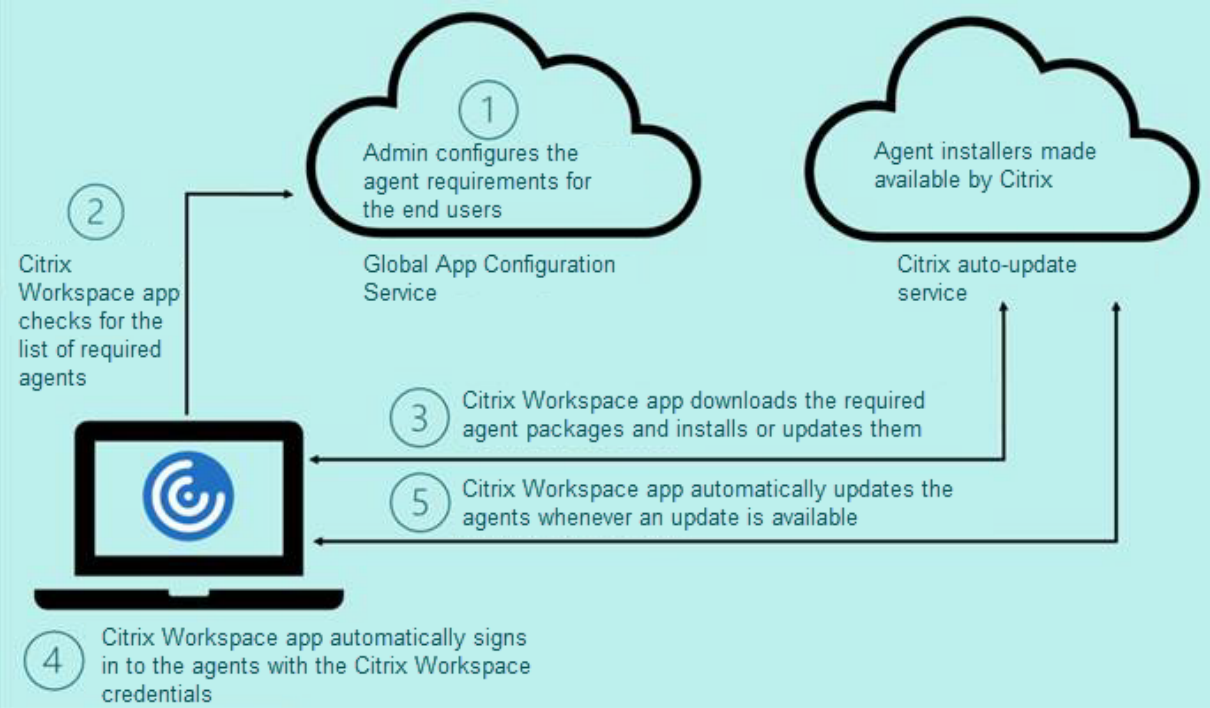
La administración de aplicaciones cliente incluye los siguientes pasos:

- Los administradores deben especificar los agentes necesarios en los dispositivos de los usuarios finales en Global App Configuration Service. Con esta versión Technical Preview, los administradores pueden especificar el agente de Secure Access y el agente de Endpoint Analysis (EPA).
- La aplicación Citrix Workspace obtiene la lista de agentes de Global App Configuration Service.
- Según la lista obtenida de Global App Configuration Service, la aplicación Citrix Workspace descarga los paquetes de agente a través del servicio de actualización automática. Si el agente no se ha instalado anteriormente en el dispositivo de punto final, la aplicación Citrix Workspace desencadena la instalación del agente. Si el agente ya está instalado, la aplicación Citrix Workspace desencadena una actualización del agente (si la versión del agente descargado es posterior a la versión instalada).

La aplicación Citrix Workspace garantiza la actualización automática de los agentes siempre que haya una actualización disponible en el futuro.

La aplicación Citrix Workspace inicia sesión automáticamente en los agentes con las credenciales de Citrix Workspace.

El siguiente diagrama ilustra el flujo de trabajo:




Puede registrarse para obtener esta versión Technical Preview a través del formulario de Podio. Envíe una solicitud y nos pondremos en contacto con usted para proporcionarle más detalles.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

#### Mejora de la actualización automática

Ahora, la aplicación Citrix Workspace admite la actualización automática cuando están habilitadas la detección del protocolo de detección automática de proxies web (WPAD) y la configuración automática de proxy (PAC).

#### Citrix Enterprise Browser

Esta versión incluye la versión 105.2.1.40 de Citrix Enterprise Browser, basada en la versión 105 de Chromium. Para obtener más información sobre Citrix Enterprise Browser, consulte la documentación de Citrix Enterprise Browser.

#### Problemas resueltos

En esta versión se han resuelto problemas para mejorar la estabilidad, la seguridad y el rendimiento general.

### 2210

#### Novedades

#### Desenfoque de fondo para la redirección de cámaras web

Ahora, la aplicación Citrix Workspace para Windows admite el desenfoque de fondo para la redirección de cámaras web. Para habilitar esta función, seleccione la casilla **Preferencias** > **Conexiones** > **Habilitar desenfoque de fondo**.

#### Mejoras en la protección de aplicaciones para aplicaciones web y SaaS en Windows 11

Esta mejora de la protección de aplicaciones optimiza la experiencia y las prestaciones de seguridad para los usuarios de aplicaciones web y SaaS en Windows 11. Esta mejora está disponible a través de Citrix Enterprise Browser para clientes de Secure Private Access.

### Protección de aplicaciones locales [Technical Preview]

Protección de aplicaciones ofrece una mayor seguridad a la hora de defender a nuestros clientes contra registradores de pulsaciones de teclas y capturas de pantalla, ya sean accidentales o maliciosas, en los dispositivos de punto final. Actualmente, las funciones de Protección de aplicaciones solo se ofrecen con los recursos de Workspace. Con Protección de aplicaciones locales, las funciones de Protección de aplicaciones se extienden a las aplicaciones locales residentes en los dispositivos de punto final. A partir de la aplicación Citrix Workspace 2210 para Windows, se puede aplicar Protección de aplicaciones a las aplicaciones locales de los dispositivos Windows.

Puede registrarse para obtener esta versión Technical Preview a través de este formulario de Podio.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

### Limitar resoluciones de vídeo

Los administradores que tienen usuarios en dispositivos de punto final clientes de bajo rendimiento pueden optar por limitar las resoluciones de vídeos entrantes o salientes para reducir el impacto de la codificación y la decodificación de vídeo en dichos dispositivos. A partir de la aplicación Citrix Workspace 2010 para Windows, puede limitar estas resoluciones mediante las opciones de configuración del cliente.

> **Nota:**
>
> Los usuarios con resoluciones restringidas afectan a la calidad general del vídeo de las conferencias, ya que el servidor de Microsoft Teams se verá obligado a utilizar la resolución con el mínimo común denominador para todos los participantes de la conferencia.

Las restricciones de llamadas están inhabilitadas de forma predeterminada en el cliente con la aplicación Citrix Workspace 2210. Para habilitarlas, los administradores deben definir estas configuraciones en el lado del cliente en HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream:

| Name | Tipo | Mandatory (Obligatorio) | Valores aceptados |
|---|---|---|---|
| EnableSimulcast | Entero | SÍ | 1-3 (configúrelo en 1) |

| Name | Tipo | Mandatory (Obligatorio) | Valores aceptados |
|---|---|---|---|
| MaxOutgoingResolution | Entero | SÍ | 180, 240, 360, 540, 720, 1080 (resoluciones compatibles con Microsoft Teams) |
| MaxIncomingResolutio | Entero | SÍ | 180, 240, 360, 540, 720, 1080 (resoluciones compatibles con Microsoft Teams) |
| MaxIncomingStreams | Entero | SÍ | 1–8 |
| MaxSimulcastLayers | Entero | SÍ | 1-3 (configúrelo en 1) |
| MaxVideoFrameRate | Entero | NO | 1–30 |
| MaxScreenshareFramel | Entero | NO | 1–15 |

Todas las claves son DWORD.

#### Citrix Enterprise Browser

Esta versión incluye la versión 105.1.1.27 de Citrix Enterprise Browser, basada en la versión 105 de Chromium. Para obtener más información sobre Citrix Enterprise Browser, consulte la documentación de Citrix Enterprise Browser.

#### Cambio de nombre de Citrix Workspace Browser

Citrix Workspace Browser se llama ahora Citrix Enterprise Browser. El esquema personalizado ahora ha cambiado de “citrixworkspace://” a “citrixbrowser://”.

La implementación de esta transición en nuestros productos y en su documentación es un proceso continuo. Agradecemos su comprensión durante esta transición.

- La interfaz de usuario del producto, el contenido del producto y las imágenes e instrucciones de la documentación del producto se actualizarán en las próximas semanas.
- Es posible que algunos elementos (como los comandos y los MSI conserven los nombres anteriores para que los scripts existentes de cliente sigan funcionando).

- Asimismo, la documentación de producto y otros recursos relacionados (como vídeos y entradas de blog) que se incluyan como enlaces en la documentación de este producto pueden contener todavía los nombres anteriores.

#### Convertir Citrix Enterprise Browser en el explorador de trabajo [Technical Preview]

Ahora puede configurar Citrix Enterprise Browser para que abra todos los enlaces y aplicaciones de trabajo o empresariales configurados por su administrador en la aplicación Citrix Workspace. Esta función proporciona una forma de abrir solo enlaces de trabajo o aplicaciones web y SaaS en Citrix Enterprise Browser.
Puede seleccionar un explorador alternativo para abrir cualquier otro enlace o aplicación que no sea de trabajo.

#### Abrir todas las aplicaciones web y SaaS a través de Citrix Enterprise Browser

A partir de esta versión, todas las aplicaciones web internas y las aplicaciones SaaS externas disponibles en la aplicación Citrix Workspace se abren en Citrix Enterprise Browser.

> **Nota:**
>
> A partir de la versión 2210 de la aplicación Citrix Workspace para Windows, la función **Abrir todas las aplicaciones web y SaaS a través de Citrix Enterprise Browser** está inhabilitada.

#### Compatibilidad con extensiones de explorador [Technical Preview]

Es posible agregar de forma segura a Citrix Enterprise Browser las extensiones que proporcione su administrador. Un administrador puede implementar, administrar y controlar las extensiones. Los usuarios finales pueden ver y usar la extensión en citrixbrowser: //extensions si es necesario. Para obtener más información y parámetros, consulte Global App Configuration Service.

> **Nota:**
>
> Esta función se halla en una versión Tech Preview únicamente accesible mediante solicitud. Para habilitarla en su entorno, complete el formulario de Podio.

Para obtener información sobre cómo configurar, consulte la documentación de Citrix Enterprise Browser.

#### Usar Global App Config Service para administrar Citrix Enterprise Browser [Technical Preview]

El administrador puede usar Global App Config Service para Citrix Workspace para entregar los parámetros de Citrix Enterprise Browser a través de un servicio administrado de forma centralizada.

Global App Config Service se ha diseñado para que los administradores puedan configurar Citrix Workspace y administrar los parámetros de la aplicación Citrix Workspace con facilidad. Esta función permite a los administradores usar Global App Configuration Service para aplicar diversos parámetros o directivas del sistema al explorador Citrix Enterprise Browser de un almacén en particular. El administrador ahora puede configurar y administrar los siguientes parámetros de Citrix Enterprise Browser mediante Global App Configuration Service:

- "Enable CWB for all apps": Convierte a Citrix Enterprise Browser en el explorador predeterminado para abrir aplicaciones web y SaaS desde la aplicación Citrix Workspace.
- "Enable save passwords": Permite o deniega a los usuarios finales la posibilidad de guardar contraseñas.
- "Enable incognito mode": Habilita o inhabilita el modo incógnito.
- "Managed Bookmarks": Permite al administrador enviar marcadores a Citrix Enterprise Browser.
- "Enable developer tools": Habilita o inhabilita las herramientas para desarrolladores en Enterprise Browser.
- "Delete browsing data on exit": Permite al administrador configurar qué datos de Citrix Enterprise Browser se eliminarán al salir.
- "Extension Install Force list": Permite al administrador instalar extensiones en Citrix Enterprise Browser.
- "Extension Install Allow list": Permite al administrador configurar una lista de extensiones permitidas que los usuarios pueden agregar a Citrix Enterprise Browser. En esta lista se utiliza Chrome Web Store.

> **Notas:**
>
> - Esta función se halla en una versión Tech Preview únicamente accesible mediante solicitud. Para habilitarla en su entorno, complete el formulario de Podio.
> - Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.
> - El par de nombre y valor distingue entre mayúsculas y minúsculas.
> - Todos los parámetros del explorador en Global App Configuration Service se encuentran en la siguiente categoría:

```
{

    "category": "browser",
    "userOverride": false,
```

```
    "assignedTo": [
    "AllUsersNoAuthentication"
    ]
 }


<!--NeedCopy-->
```

> - El administrador también puede aplicar los parámetros a dispositivos no administrados. Para obtener más información, consulte la documentación de Global App Configuration Service.

**Problemas resueltos**

- Se vuelve a introducir el menú **PPP elevado** en **Preferencias avanzadas**.
  - El nuevo valor predeterminado es **No, usar la resolución nativa**, también conocido como correspondencia de PPP.

    Al seleccionar esta opción, la aplicación Citrix Workspace intenta corresponder automáticamente la resolución de la pantalla y los parámetros del escalado de PPP del cliente Windows local con la sesión de Citrix. Se recomienda usar la correspondencia de PPP en todos los casos, especialmente cuando se utilizan monitores de alta resolución (superiores a 1920 x 1080).
  - La opción **Sí**, también conocida como modo de compatibilidad o escalado del lado del cliente, solo se recomienda para aplicaciones antiguas, sin reconocimiento de PPP, y solo debe usarse en circunstancias especiales. Esta opción podría tener algunos efectos colaterales al mostrar las aplicaciones antiguas, como texto borroso debido a la ampliación de escala o ajuste de la sesión HDX.

    También es una opción viable cuando dos monitores con diferentes configuraciones de PPP (o valor de PPP mixto) están conectados al cliente local Windows.

    > **Nota:**
    >
    > Esta opción no es compatible con la optimización de HDX para Microsoft Teams.
  - Con la tercera opción, **Dejar que el sistema operativo ajuste la resolución**, conocida también como sin reconocimiento de PPP, la aplicación Citrix Workspace para Windows ignora la configuración de escala de PPP en el cliente local Windows. En este modo, el sistema operativo Windows debe administrar el escalado de la aplicación Workspace y la sesión HDX, igual que con cualquier otra aplicación sin reconocimiento de PPP. No se recomienda utilizar este modo con escalas de PPP superiores al 100%.

[HDX-43720]

- Al agregar un almacén inhabilitado mediante GPO y un almacén diferente del mismo servidor de StoreFront mediante la GUI, es posible que aparezca una pantalla de carga y que no se pueda agregar una cuenta. [CVADHELP-20776]
- Al agregar dos almacenes del mismo servidor de StoreFront mediante GPO, la configuración del segundo almacén podría fallar de forma intermitente. [CVADHELP-20655]
- La aplicación Citrix Workspace intenta conectarse al servidor de Global App Config, incluso cuando la directiva de Global App Config Service está inhabilitada mediante GPO. [CVADHELP-20775]
- Al usar la aplicación Citrix Workspace para Windows 2106 o una versión posterior, es posible que la funcionalidad de proxy ICA saliente no funcione. [CVADHELP-20824]
- Para los usuarios del dominio, el proceso receiver.exe puede fallar de forma imprevista. Es posible que vea este problema en la aplicación Citrix Workspace para Windows 2206 o en una versión posterior. [CVADHELP-20986]
- En la videoconferencia optimizada de Microsoft Teams, en la unión a llamada con vídeo activado, es posible que una llamada se desconecte. Este problema ocurre de forma esporádica y cuando el proceso HdxRtcEngine.exe falla en el lado del cliente. [CVADHELP-21095]

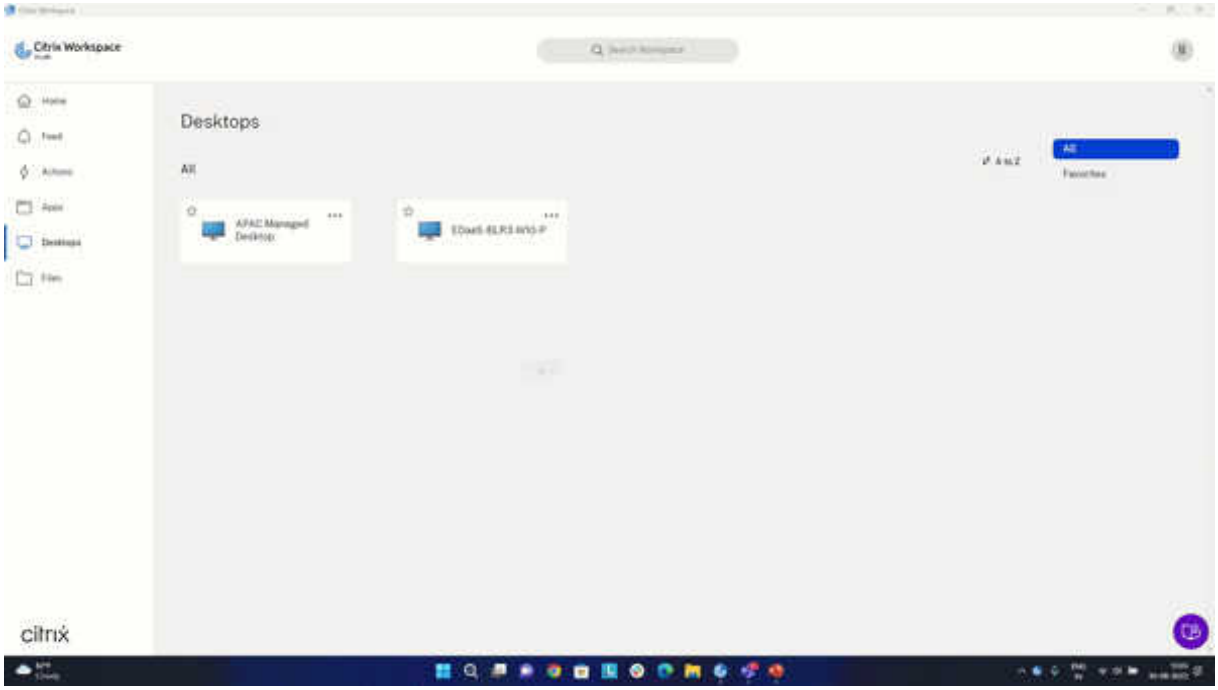
## 2209

### Novedades

#### Inicio rápido de escritorios desconectados [Technical Preview]

Al habilitar esta función, puede abrir al instante escritorios que estaban desconectados. Una vez habilitada esta función, la aplicación Citrix Workspace inicia las sesiones desconectadas en modo oculto. La sesión se presenta al instante en cuanto se abre el escritorio.




> **Nota:**
>
> Esto solo se aplica a las sesiones de Workspace (en la nube).

Puede registrarse para obtener esta versión Technical Preview a través del formulario de Podio.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

#### Control de versiones de actualizaciones automáticas [Technical Preview]

Ahora, los administradores pueden administrar la versión de las actualizaciones automáticas de los dispositivos de la organización.

Los administradores pueden controlar la versión al establecer el intervalo en las propiedades maximumAllowedVersion y minimumAllowedVersion de Global App Config Service.

Ejemplo de archivo JSON en Global App Config Service:

```
1 "AutoUpdate": {
2
3 "userOverride": false,
```

```
"AutoUpdatePluginsSettings": [
    {

    "pluginSettings": {

      "upgradeToLatest": false,
      "maximumAllowedVersion": "22.9.0.3934",
      "minimumAllowedVersion": "22.9.0.3934",
          }
 ,
    "pluginName": "WorkspaceApp",
    "pluginId": "1CDF566D-B2C7-47CA-802F-6283C862E1D6"
   }


<!--NeedCopy-->
```

Al establecer el intervalo, la aplicación Citrix Workspace del dispositivo del usuario se actualiza automáticamente a la versión más reciente disponible que se encuentre en el intervalo mencionado.

Si quiere actualizar automáticamente la aplicación Citrix Workspace a una versión específica, introduzca la misma versión en las propiedades maximumAllowedVersion y minimumAllowedVersion de Global App Config Service.

> **Nota:**
>
> - Para efectuar el control de versiones de las actualizaciones automáticas, el parámetro upgradeToLatest de Global App Config Service debe estar establecido en false. Si es true, se ignorarán maximumAllowedVersion y minimumAllowedVersion.
> - No modifique pluginId, ya que está asignado a la aplicación Citrix Workspace.
> - Si el administrador no ha configurado la versión en Global App Config Service, la aplicación Citrix Workspace se actualiza a la versión disponible más reciente de forma predeterminada.

Para habilitar esta funcionalidad:

1. Abra el Editor del Registro.
2. Vaya a la ruta del Registro `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle`.
3. Cree un valor del Registro con estos atributos:
    - Nombre de la clave del Registro: Test-EnableAUVersionControl
    - Tipo: DWORD
    - Valor: 0 es inhabilitado, y si es mayor que 0, está habilitado

4. Reinicie la aplicación Citrix Workspace para que los cambios surtan efecto.

Puede enviar comentarios sobre esta función a través del formulario de Podio.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

#### Versión mejorada de WebRTC para Microsoft Teams optimizado

La versión de WebRTC que se utiliza para Microsoft Teams optimizado se ha actualizado a la versión M98.

#### Función de actualización automática de la aplicación Citrix Workspace en VDA

Ahora puede habilitar la función de actualización automática en el VDA mediante la creación de este valor del Registro:

En una máquina de 32 bits:

- Clave del Registro: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\AutoUpdate
- Valor del Registro: AllowAutoUpdateOnVDA
- Tipo de Registro: REG_SZ
- Datos del Registro: True

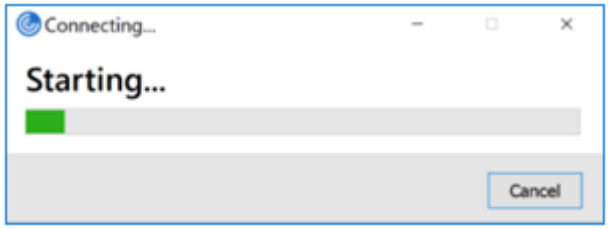
En una máquina de 64 bits:

- Clave del Registro: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\AutoUpdate
- Valor del Registro: AllowAutoUpdateOnVDA
- Tipo de Registro: REG_SZ
- Datos del Registro: True

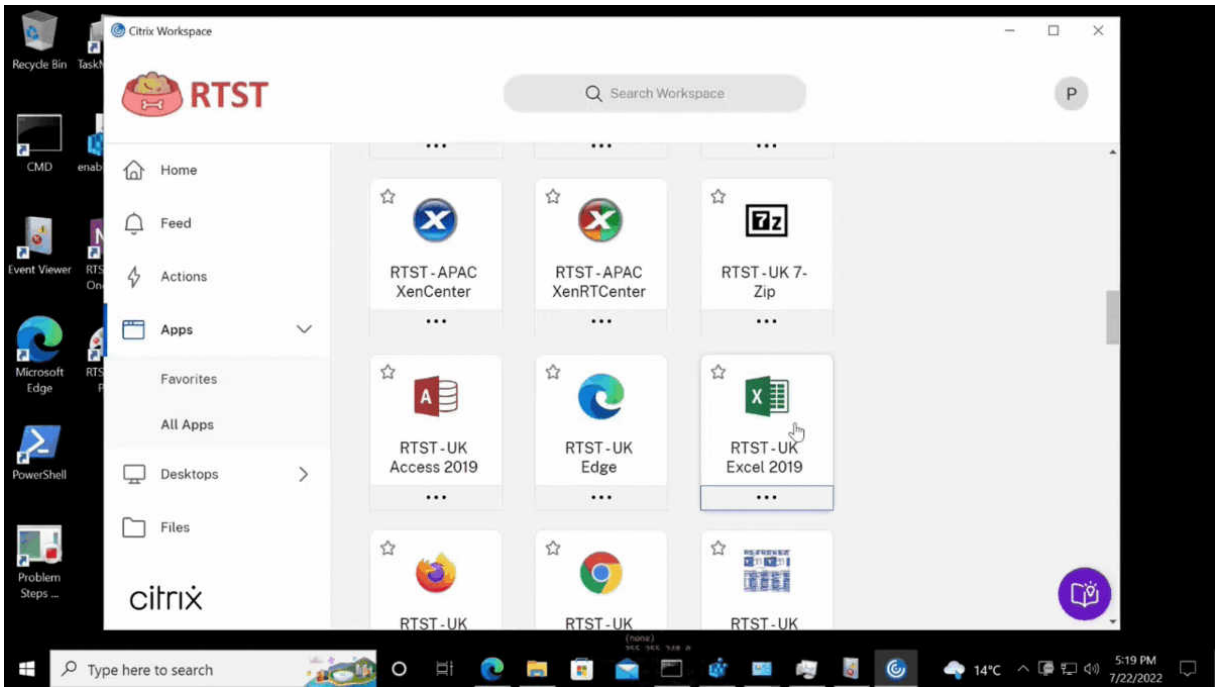
#### Experiencia mejorada al iniciar aplicaciones y escritorios virtuales [Technical Preview]

Antes, el cuadro de diálogo de progreso del inicio no era intuitivo para los usuarios. Les hacía creer que el proceso de inicio no respondía, y estos cerraban el cuadro de diálogo, ya que los mensajes de notificación eran estáticos.

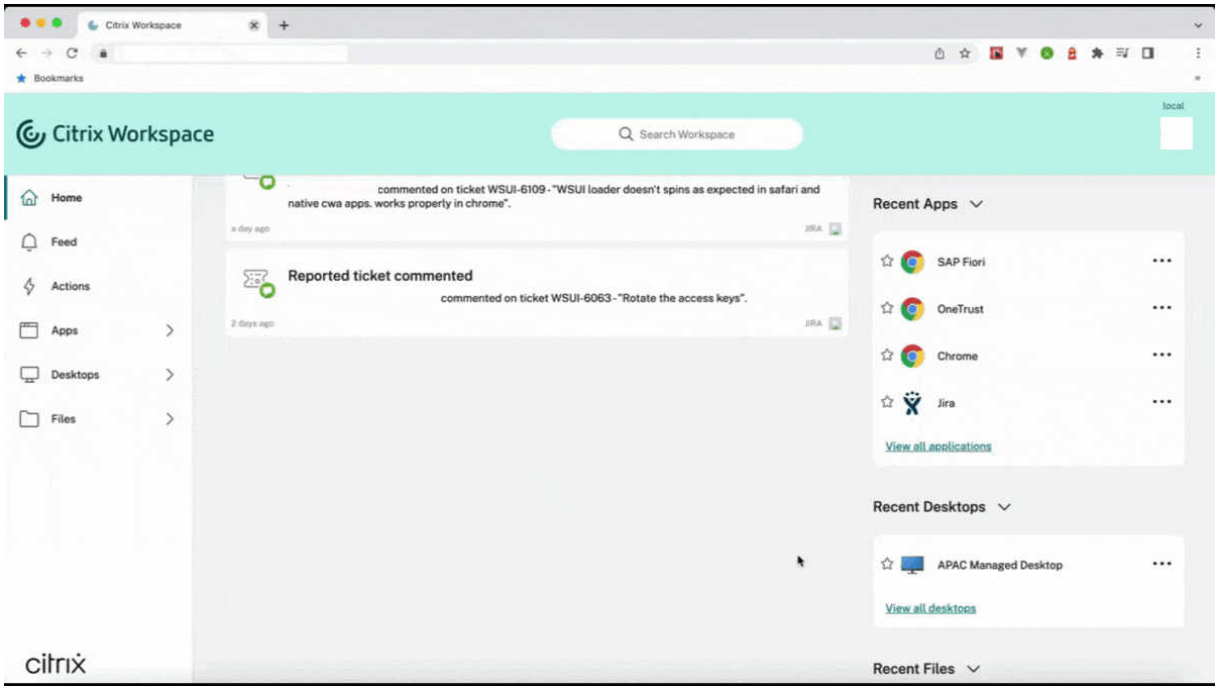



La experiencia mejorada al iniciar aplicaciones y escritorios es más informativa, moderna e intuitiva en la aplicación Citrix Workspace para Windows. Esto ayuda a mantener a los usuarios informados con datos relevantes y oportunos sobre el estado del inicio. La notificación aparece en la esquina inferior derecha de la pantalla.




Esta función también está disponible en Workspace para Web. Los usuarios pueden ver notificaciones útiles sobre el progreso del inicio en lugar de un icono giratorio solamente. Si hay un inicio en curso y el usuario intenta cerrar el explorador, aparece un mensaje de advertencia.




Puede habilitar esta función mediante el Registro:

1. Abra el Editor del Registro.
2. Vaya a `HKLM\SOFTWARE\WOW6432Node\Citrix\Dazzle`.
3. Cree y agregue una cadena del Registro con el nombre NewLaunchExpSupport, y establezca su valor en True.
4. Reinicie la aplicación Citrix Workspace para que los cambios surtan efecto.

> **Nota:**
>
> Esto solo se aplica a las sesiones de Workspace (en la nube).

**Problemas conocidos:**

- En una configuración con varios monitores, las ventanas de aplicaciones en una sesión de escritorio de la aplicación Citrix Workspace se mueven a un monitor diferente. Este problema se produce cuando se desconecta de una sesión y se conecta a ella de nuevo.
- Esta función no está disponible en el inicio por explorador web.

Puede enviar comentarios sobre esta función a través del formulario de Podio.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta

> en entornos de producción.

**Citrix Enterprise Browser (antes denominado Citrix Workspace Browser)**

Esta versión incluye la versión 103.2.1.10 de Citrix Enterprise Browser, basada en la versión 103 de Chromium. Para obtener más información sobre Citrix Enterprise Browser, consulte la documentación de Citrix Enterprise Browser.

- **Perfiles de Citrix Enterprise Browser**

  Los perfiles le ayudan a mantener información personal, como el historial, los marcadores, las contraseñas y otros parámetros, por separado para cada una de sus cuentas de Citrix Workspace. En función de su almacén de Workspace, se crea un perfil que le permite disfrutar de una experiencia de navegación única y personalizada.

  > **Nota:**
  >
  > Después de actualizar la versión a 103.2.1.10 e iniciar sesión en el dispositivo por primera vez, solo se quitarán las contraseñas guardadas anteriormente. Al iniciar sesión en el dispositivo en un almacén diferente por primera vez, se pierden todos los datos guardados anteriormente.

**Problemas resueltos**

- Con esta corrección, aparece una página de inicio de sesión al cerrar la sesión de la aplicación Citrix Workspace para Windows, específica para almacenes locales.

  Para habilitar la corrección, defina estos valores del Registro:

  En sistemas de 32 bits:

  - HKEY_LOCAL_MACHINE/Software/Citrix/Dazzle
  - Nombre: ShowSignInPageOnLogOff
  - Tipo: REG_SZ
  - Valor: True

  En sistemas de 64 bits:

  - HKEY_LOCAL_MACHINE/Software/Wow6432Node/Citrix/Dazzle
  - Nombre: ShowSignInPageOnLogOff
  - Tipo: REG_SZ
  - Valor: True

  [CVADHELP-19967]

- La regla AppLocker del objeto de directiva de grupo bloquea la integración del plug-in de Citrix Gateway en Citrix Workspace. Como resultado, se crean varios archivos temporales con el

formato VPNXXXX.tmp en la carpeta temporal. Los archivos se crean incluso cuando la clave del Registro, HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client, tiene el valor DisableIconHide. [CVADHELP-19709]

- Al iniciar una aplicación publicada a través de un sitio de PNAgent, la aplicación Citrix Workspace para Windows muestra este mensaje:

  **Ocurrió un error fatal.**

  [RFWIN-28208]

- Es posible que la aplicación Citrix Workspace no responda después del inicio. {CVADHELP-20317]

## 2207

### Novedades

#### Efectos y desenfoque de fondo para la optimización de Microsoft Teams con HDX

Ahora, la aplicación Citrix Workspace para Windows admite efectos y el desenfoque de fondo en la optimización de Microsoft Teams con HDX.

Puede difuminar o reemplazar el fondo por una imagen personalizada y evitar distracciones inesperadas al ayudar a que la conversación se centre en la silueta (cuerpo y rostro). La función se puede utilizar con llamadas de conferencia o entre dos usuarios.

> **Nota:**
>
> Ahora, esta función está integrada en los botones y la interfaz de usuario de Microsoft Teams. La compatibilidad con varias ventanas es un requisito previo que necesita una actualización de VDA a la versión 2112 o a una posterior. Para obtener más información, consulte Reuniones y chat en modo multiventana.

**Limitaciones:**

- No se admite el reemplazo de fondo definido por el administrador y el usuario.
- El efecto de fondo no persiste entre sesiones. Cuando cierra y reinicia Microsoft Teams o el VDA se conecta de nuevo, el efecto de fondo se restablece y se desactiva.
- Cuando la sesión ICA se conecta de nuevo, el efecto está desactivado. Sin embargo, la interfaz de usuario de Microsoft Teams muestra que el efecto anterior sigue activado con una marca de verificación. Citrix y Microsoft están trabajando juntos para resolver este problema.
- El dispositivo debe estar conectado a Internet mientras se reemplaza la imagen de fondo.

> **Nota:**
>
> Esta función estará disponible solamente después de la implantación de una futura actualización de Microsoft Teams. Cuando Microsoft implante la actualización, puede consultar CTX253754 y

> el Plan de desarrollo público de Microsoft 365 para obtener información sobre el anuncio y la actualización de la documentación.

**Desenfoque de fondo para la redirección de cámaras web [Technical Preview]**

Ahora, la aplicación Citrix Workspace para Windows admite el desenfoque de fondo para la redirección de cámaras web. Puede habilitar esta función mediante el Registro:

- Ubicación: HKCU\Software\Citrix\HdxRealTime.
- Nombre: EnableBackgroundEffectFilter.
- Tipo: DWORD.
- Valor: 0 es inhabilitado. Se habilita cualquier otro valor. Si el valor no existe o es 0, se omiten todos los parámetros de desenfoque de fondo, y se inhabilita la casilla **Preferencias** > **Conexiones** > **Habilitar desenfoque de fondo** que gestiona el efecto de desenfoque.

**Recomendación:**

Cierre la aplicación de la cámara web en el VDA antes de cerrar la sesión ICA.

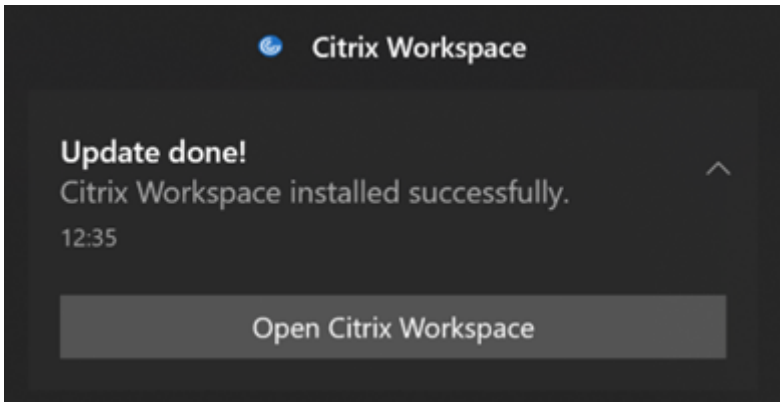
Puede enviar comentarios sobre esta función a través del formulario de Podio.

**Experiencia de actualización automática mejorada**

La función de actualización automática actualiza automáticamente la aplicación Citrix Workspace a la versión más reciente sin necesidad de la intervención del usuario.

La aplicación Citrix Workspace comprueba periódicamente y descarga la versión más reciente disponible de la aplicación. La aplicación Citrix Workspace determina el mejor momento para la instalación en función de la actividad del usuario para no provocar ninguna interrupción.

Cuando se complete la instalación, aparecerá esta notificación:




Si la aplicación Citrix Workspace no encuentra el momento adecuado para instalar las actualizaciones en segundo plano, aparece una notificación.

#### Mejora de la actualización automática [Technical Preview]

Ahora, la aplicación Citrix Workspace admite la actualización automática cuando están habilitadas la detección del protocolo de detección automática de proxies web (WPAD) y la configuración automática de proxy (PAC).

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Puede enviar comentarios sobre esta función a través del formulario de Podio.

### Citrix Enterprise Browser

Esta versión incluye la versión 102.1.1.14 de Citrix Enterprise Browser, basada en la versión 102 de Chromium.

- **Abra todas las aplicaciones web y SaaS a través de Citrix Enterprise Browser [Technical Preview]**

  A partir de esta versión, todas las aplicaciones web internas y las aplicaciones SaaS externas disponibles en la aplicación Citrix Workspace se abren en Citrix Enterprise Browser. Puede registrarse para obtener esta versión Technical Preview a través del formulario de Podio.

  > **Nota:**
  >
  > Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

### Nota sobre la actualización de la aplicación Citrix Workspace

Al actualizar la aplicación Citrix Workspace para Windows de la versión anterior a la versión 2207, se le pide al usuario que inicie sesión. El inicio de sesión solo se solicita para el almacén del espacio de trabajo.

### Problemas resueltos

#### Sesión/Conexión

- Es posible que Microsoft Teams optimizado no seleccione un nuevo dispositivo de audio predeterminado conectado al dispositivo de punto final. [CVADHELP-20528]

  > **Nota:**
  >
  > Esta corrección estará disponible solamente después de la implantación de una futura actualización de Microsoft Teams.

- Es posible que la configuración de almacenes mediante direcciones URL con DNS geográfico a través de un objeto de directiva de grupo o la línea de comandos no funcione si estableció AllowAddStore=N durante la instalación de la aplicación Citrix Workspace. [CVADPHELP-19853]
- Es posible que Citrix Authentication Manager (AuthManSvr.exe) se cierre de forma inesperada durante el inicio de sesión. [CVADHELP-18901]

#### Interfaz de usuario

- Cuando usa almacenes web personalizados, los enlaces de la aplicación Citrix Workspace se abren en el explorador web del sistema. [RFWIN-27855]

## 2206

### Novedades

#### Efectos y desenfoque de fondo para la optimización de Microsoft Teams con HDX [Technical Preview]

En la aplicación Citrix Workspace 2206 para Windows, Citrix presenta una versión Tech Preview para los efectos y el desenfoque de fondo en la optimización de Microsoft Teams con HDX.

Ahora, puede difuminar o reemplazar el fondo por una imagen personalizada y evitar distracciones inesperadas al ayudar a que la conversación se centre en la silueta (cuerpo y rostro). La función se puede utilizar con llamadas de conferencia o entre dos usuarios.

> **Nota:**
>
> - En esta versión Tech Preview, la función solo se puede controlar a través de las claves del Registro y no está integrada en la interfaz de usuario ni los botones de Microsoft Teams.
> - El nuevo fondo persiste en todas las reuniones y llamadas de Microsoft Teams hasta que lo cambie de nuevo mediante una clave del Registro. Para que el cambio surta efecto, solo debe reiniciar Microsoft Teams. Esta limitación desaparece cuando la función está disponible de forma general y, para ello, se necesita la función de ventanas múltiples (VDA

> 2112 o una versión posterior).
> Para activar o desactivar los efectos y el desenfoque de fondo, los administradores o los usuarios deben configurar esta clave del Registro en el cliente o dispositivo de punto final:

Ubicación: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Nombre: VideoBackgroundEffect
- Tipo: DWORD
- Valor: 0 (inhabilitado), 1 (habilitado), 2 (reemplazo de imagen de fondo, lo que requiere que la clave **VideoBackgroundImage** también esté presente)

Esta clave solo es necesaria si quiere reemplazar la imagen de fondo, no desenfocarla:

- Nombre: VideoBackgroundImage
- Tipo: REG_SZ
- Valor: nombre_de_imagen.jpeg

> **Nota:**
>
> El nombre del archivo (por ejemplo: nombre_de_imagen.jpg o el nombre que proporcione al archivo) debe colocarse en el dispositivo del usuario, en el directorio de instalación de la aplicación Citrix Workspace: `C:\Program Files (x86)\Citrix\ICA Client`.

#### Rendimiento gráfico mejorado

La aplicación Citrix Workspace 2206 presenta importantes mejoras de rendimiento para las GPU integradas de Intel:

- Se ha reducido el consumo de GPU para los gráficos, lo que mejora el rendimiento general.

Se han solucionado estos problemas:

- Un nivel bajo de fotogramas por segundo después de reproducir un vídeo en la GPU de Intel de 10.ª generación o una posterior.
- Diferencia de brillo en la opción gradual sin pérdida o para las regiones que cambian activamente en las GPU de Intel y AMD.

#### Mejora de la protección de aplicaciones: Antiinyección de código [Technical Preview]

Ahora, la aplicación Citrix Workspace garantiza que ninguna biblioteca de enlaces dinámicos (DLL) no autorizada ni módulos que no sean de confianza puedan acceder a la sesión.

Si se inyecta algún módulo que no sea de confianza durante una sesión, la aplicación Citrix Workspace detecta dicha intervención e impide que se cargue el módulo.

Además, si se detecta alguna DLL maliciosa o que no sea de confianza antes del inicio de la sesión, la protección de aplicaciones bloquea el inicio de la sesión y muestra un mensaje de error. Al cerrar el mensaje de error, se cierra la sesión de escritorio y aplicación virtual.

Puede registrarse para obtener esta versión Technical Preview a través de este formulario de Podio.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

**Mejoras en la protección de aplicaciones para aplicaciones web y SaaS en Windows 11 [Technical Preview]**

Esta mejora de la protección de aplicaciones optimiza la experiencia y las prestaciones de seguridad para los usuarios de aplicaciones web y SaaS en Windows 11. Esta mejora está disponible a través de Citrix Enterprise Browser para clientes de Secure Private Access. Puede registrarse en la Technical Preview a través del formulario de Podio. Para obtener más información, consulte Protección de aplicaciones.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

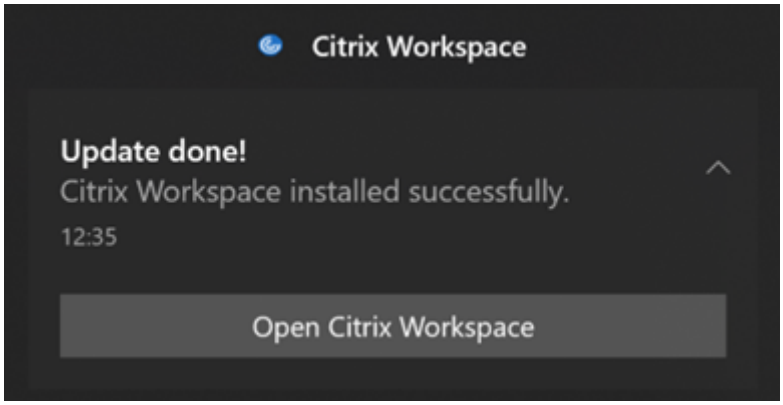
**Mejora de la experiencia de actualización automática [Technical Preview]**

La función de actualización automática actualiza automáticamente la aplicación Citrix Workspace a la versión más reciente sin necesidad de la intervención del usuario.

La aplicación Citrix Workspace comprueba periódicamente y descarga la versión más reciente disponible de la aplicación. La aplicación Citrix Workspace determina el mejor momento para la instalación en función de la actividad del usuario para no provocar ninguna interrupción.

Cuando se complete la instalación, aparecerá esta notificación:




Si la aplicación Citrix Workspace no encuentra el momento adecuado para instalar las actualizaciones en segundo plano, aparece una notificación.

Puede registrarse en la Technical Preview a través del formulario de Podio.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

#### Habilitar la correspondencia de PPP

A partir de la aplicación Citrix Workspace 2206 para Windows, la correspondencia de PPP está habilitada de forma predeterminada. Esto significa que la aplicación Citrix Workspace intenta corresponder automáticamente la resolución de la pantalla y los parámetros del escalado de PPP del cliente Windows local con la sesión de Citrix. Como parte de este cambio, la opción de PPP elevados disponible en Preferencias avanzadas de la aplicación Citrix Workspace ya no está disponible. Para obtener más información, consulte el artículo CTX460068 de Citrix Knowledge Center.

#### Citrix Enterprise Browser

Esta versión incluye la versión 101.1.1.12 de Citrix Enterprise Browser, basada en la versión 101 de Chromium. Para ver las funciones o correcciones de errores de Citrix Enterprise Browser, consulte Novedades en la documentación de Citrix Enterprise Browser.

#### Problemas resueltos

#### Instalación, desinstalación, actualización de versiones

- Es posible que Citrix Workspace Updater Service no se inicie y se produzca un error de instalación. Este problema se produce cuando el cliente no está conectado a Internet. [CVADHELP-19613]

### Sesión/Conexión

- Al usar la aplicación Citrix Workspace 2204.1 o una versión posterior, es posible que la sesión se desconecte. Este problema se produce si hay una restricción para ejecutar binarios sin firmar, como, por ejemplo, wfica.ocx. [CVADHELP-20053]
- Al iniciar la aplicación Citrix Workspace por primera vez después de agregar la URL del almacén, aparece este mensaje de error:

  "Su aplicación Citrix Workspace encontró un error al inicializar Microsoft Edge WebView2. Reinicie la aplicación".

  Este problema se produce al agregar la URL del almacén a través de GPO o la línea de comandos, e incluye "/" tras la detección. Por ejemplo: `https://sales.example.com/Citrix/Store/discovery/;On;Store`.

  [CVADHELP-20214]
- En la aplicación Citrix Workspace para Windows, al agregar direcciones URL de almacén mediante el objeto de directiva de grupo, es posible que aparezca este mensaje de error:
  "No se puede conectar con el servidor".

  Este problema se produce si uno de los almacenes está inhabilitado y no se puede acceder a él. [CVADHELP-19751]
- Al actualizar la aplicación Citrix Workspace desde la versión 2006 o una anterior, es posible que se eliminen las configuraciones de puerta de enlace y baliza de los almacenes existentes y se agreguen de nuevo las mismas configuraciones aunque las configuraciones de almacén no se modifican en el objeto de directiva de grupo. [CVADHELP-19839]
- Es posible que no se puedan iniciar aplicaciones o escritorios desde una tableta con la aplicación Citrix Workspace. El problema se produce cuando no se puede obtener la dirección IP del cliente. [CVADHELP-19703]
- Mientras comparte la pantalla o una aplicación durante llamadas de Microsoft Teams, es posible que sus compañeros vean artefactos visuales. Este problema se produce por velocidades de fotogramas inestables, como una reproducción de vídeo incorrecta (fotogramas negros congelados o transitorios). Esta versión incluye velocidades de fotogramas o de muestreo mejoradas que ayudan a reducir los artefactos visuales. [HDX-38032]

### Interfaz de usuario

- Es posible que la barra de herramientas de **Desktop Viewer** no se vea al abrir el escritorio virtual desde almacenes de portales personalizados. [CVADHELP-20253]
- Al usar la aplicación Citrix Workspace para Windows con Redirección de contenido del explorador, el cambio de tamaño de la ventana del explorador continúa aunque suelte el botón del mouse. [HDX-38024]
- Es posible que la notificación del estado de la batería y el cuadro de diálogo emergente del teclado automático no aparezcan durante la sesión cuando la directiva Visualización automática del teclado está habilitada en el DDC. [HDX-39558]
- Al conectar un dispositivo USB o acceder a archivos, es posible que la aplicación Citrix Workspace muestre el cuadro de diálogo antiguo **Citrix Workspace: Advertencia de seguridad**. [LCM-10369]

#### Continuidad del servicio

- Es posible que no se pueda iniciar la aplicación Citrix Workspace por falta de archivos de concesión, lo que provoca el error 3002. Esta versión incluye una mejora en la que la sincronización de concesiones se completa solo cuando el cliente sincroniza todos los archivos de concesión presentes en el servidor. [RFWIN-26540]

### 2205

#### Novedades

> **Nota:**
>
> A partir de esta versión, asegúrese de que la versión de Microsoft Edge WebView2 Runtime sea 99 o una posterior. Para obtener más información, consulte Requisitos del sistema y compatibilidad.

#### Cambio en Citrix Casting

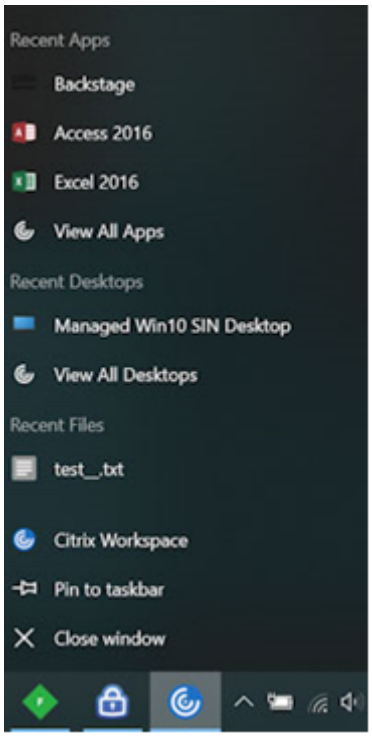
Antes, Citrix Casting estaba habilitado de forma predeterminada durante la instalación de la aplicación Citrix Workspace. A partir de esta versión, Citrix Casting solo se habilita si ejecuta el instalador de la aplicación Citrix Workspace con el comando `/IncludeCitrixCasting` durante la instalación. Al actualizar la aplicación Citrix Workspace, Citrix Casting se actualiza automáticamente. Para obtener más información sobre Citrix Casting, consulte Citrix Casting.

#### Acceso rápido a recursos

A partir de esta versión, puede obtener acceso rápido a aplicaciones, escritorios y archivos que haya utilizado recientemente. Haga clic con el botón secundario en el icono de la aplicación Citrix

Workspace de la barra de tareas para ver y abrir los recursos utilizados recientemente en el menú emergente.




#### Cerrar sesión en el almacén web personalizado al salir de la aplicación Citrix Workspace

Cuando el atributo `signoutCustomWebstoreOnExit` tiene el valor True, al cerrar la aplicación Citrix Workspace se cierra la sesión en los almacenes web personalizados. Puede configurar el atributo `signoutCustomWebstoreOnExit` en **Global App Configuration Service**.

Para obtener más información, consulte la documentación de Global App Configuration Service.

#### Función para abrir la aplicación Workspace en modo maximizado

A partir de esta versión, puede optar por abrir la aplicación Citrix Workspace en modo maximizado. En lugar de maximizar la aplicación Citrix Workspace de forma manual cada vez, puede establecer la propiedad `maximise workspace window` en Global App Configuration Service para permitir que la aplicación Workspace se abra en modo maximizado de forma predeterminada.

Para obtener más información sobre Global App Configuration Service, consulte Getting Started.

#### Función Storebrowse para Workspace

Ahora, la aplicación Citrix Workspace para Windows permite usar Storebrowse para el autoservicio, lo que permite a los usuarios de Storebrowse acceder a las funciones de Cloud y Workspace.

> **Nota:**
>
> - Esta función permite usar Storebrowse solamente con Single Sign-On.
> - Los requisitos previos mencionados en Requisitos y compatibilidad del sistema deben estar disponibles para usar esta función.

Para obtener más información, consulte Storebrowse para Workspace.

### Citrix Enterprise Browser

- Esta versión incluye la versión 99.1.1.8 de Citrix Enterprise Browser, basada en la versión 99 de Chromium. Para ver las funciones o correcciones de errores de Citrix Enterprise Browser, consulte Novedades en la documentación de Citrix Enterprise Browser.
- Ahora, la aplicación Citrix Workspace le avisa sobre el cierre de ventanas activas del explorador web al hacer una de estas acciones en la aplicación Citrix Workspace:
  - Cerrar la sesión de un almacén
  - Cambiar a otro almacén
  - Agregar un nuevo almacén
  - Eliminar el almacén actual

## Problemas resueltos

### Interfaz de usuario

- En la aplicación Citrix Workspace para Windows, es posible que los usuarios que no son administradores no puedan inhabilitar el parámetro **Recopilación de datos** a través del cuadro de diálogo **Preferencias avanzadas**. [RFWIN-26795]

### Sesión/Conexión

- Al reiniciar Microsoft Teams, es posible que el proceso HdxRtcEngine.exe existente no se cierre y que se inicie un nuevo proceso. [HDX-40006]
- Durante llamadas entre dos usuarios con la optimización HDX de Microsoft Teams, es posible que el uso compartido de la ventana de una aplicación no se detenga después de iniciar y detener el uso compartido muchas veces, y es posible que no pueda compartir la pantalla del escritorio ni la ventana de la aplicación ni llamar ni recibir llamadas hasta que haya reiniciado la aplicación Citrix Workspace. [HDX-39549]
- Durante la sesión de Dar control con la optimización HDX de Microsoft Teams, el cursor remoto aparece ligeramente desplazado de su posición real. [HDX-36376]

- Cuando accede a un VDA por primera vez con la versión 2112 de la aplicación Citrix Workspace para Windows o una posterior, es posible que aparezca este mensaje de seguridad:

  **Una aplicación conectada está intentando acceder a la información en un dispositivo conectado al acceso a archivos HDX de su equipo.**

  En versiones anteriores, este mensaje solo aparecía durante el primer acceso a cada recurso publicado en un grupo de entrega y no en todos los VDA.

  [CVADHELP-19636]

#### Instalación, desinstalación, actualización de versiones

- Al actualizar la versión de la aplicación Citrix Workspace para Windows, es posible que se cree esta clave de Registro adicional:

  `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\WOW6432Node\Citrix`

  El problema se produce cuando se configura la directiva de línea de comandos de actualización automática.

  El valor del Registro TransparentKeyPassthrough de `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard` no se conserva en máquinas de 32 bits.

  [CVADHELP-19625]

### 2204.1

#### Novedades

#### Mejora en la redirección de audio

Compatibilidad mejorada con eliminación de eco en todos los códecs de audio, incluidos los códecs de audio adaptable y todos los códecs de audio antiguos.

#### Compatibilidad con una experiencia mejorada de Single Sign-On (SSO) para aplicaciones web y SaaS [Technical Preview]

Esta función simplifica la configuración de SSO para aplicaciones web y SaaS internas al usar proveedores de identidades (IdP) de terceros. La experiencia mejorada de SSO reduce todo el proceso a unos pocos comandos. Elimina el requisito previo obligatorio de configurar Citrix Secure Private Access en la cadena de IdP para configurar SSO. También mejora la experiencia del usuario, siempre que se utilice el mismo IdP para la autenticación tanto en la aplicación Workspace como en la aplicación web o SaaS correspondiente que se inicie.

Puede registrarse para obtener esta versión Technical Preview a través de este formulario de Podio.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

#### Citrix Enterprise Browser

Esta versión incluye la versión 98.1.2.20 de Citrix Enterprise Browser, basada en la versión 98 de Chromium. Para ver las funciones o correcciones de errores de Citrix Enterprise Browser, consulte Novedades en la documentación de Citrix Enterprise Browser.

#### Optimización de Microsoft Teams

- **Compatibilidad con timbre secundario**: Puede utilizar la función de **timbre secundario** para seleccionar un dispositivo secundario en el que recibir la notificación de llamada entrante cuando Microsoft Teams está optimizado (Citrix HDX optimizado en Acerca de/Versión). Por ejemplo, si ha configurado un altavoz como **timbre secundario** y el dispositivo de punto final está conectado a unos auriculares, Microsoft Teams envía la señal de llamada entrante al altavoz aunque los auriculares sean el periférico principal para la llamada de audio. Si no está conectado a más de un dispositivo de audio o si el periférico no está disponible (por ejemplo, auriculares Bluetooth), no puede configurar un timbre secundario.

  > **Nota:**
  >
  > Esta función estará disponible solamente después de la implantación de una futura actualización de Microsoft Teams. Para saber cuándo implementa Microsoft la actualización, consulte el Plan de desarrollo de Microsoft 365. También puede consultar CTX253754 para obtener la actualización de la documentación y el anuncio.

- **Mejora en Protección de aplicaciones y Microsoft Teams**: Microsoft Teams admite el uso compartido de pantallas y vídeos entrantes cuando la aplicación Citrix Workspace para Windows con Protección de aplicaciones habilitada está en modo Desktop Viewer únicamente. Las aplicaciones publicadas en modo integrado no representan el vídeo entrante ni las pantallas compartidas.

### Problemas resueltos

#### Sesión/Conexión

- Es posible que el dispositivo Citrix ADC se cierre de forma inesperada cuando se dan ciertas condiciones en la aplicación Citrix Workspace para Windows. [HDX-39683]
- En la aplicación Citrix Workspace, es posible que se produzcan errores intermitentes al responder o realizar llamadas de Microsoft Teams. Aparece el siguiente mensaje de error:

**No se pudo establecer la llamada.**

[HDX-38819]

- Cuando intenta redirigir hacia la cámara web preferida conforme a la configuración establecida en la aplicación Citrix Workspace para Windows, es posible que no funcione del modo previsto.

  Con esta corrección, la cámara web preferida será la única cámara web disponible en la sesión de usuario. De esta forma, se logra un mayor control cuando hay varias cámaras web disponibles en la sesión de usuario.

  [HDX-38214]

- Si la aplicación Citrix Workspace está configurada para mostrar aplicaciones en la carpeta de acceso directo del menú **Escritorio e Inicio**, es posible que, al iniciar sesiones de aplicaciones y escritorios desde el menú **Escritorio o Inicio** después de cerrar la aplicación Citrix Workspace, se produzca un error. [RFWIN-26508]
- Es posible que, de manera intermitente, no se pueda agregar la dirección URL de Citrix Gateway y se muestre el siguiente mensaje de error:

  **No se pudo establecer contacto con el servicio de autenticación.**

  [CVADHELP-19415]

- Con esta corrección, puede configurar **TWITaskbarGroupingMode** en **GroupNone**, tanto en `HKEY_CURRENT_USER` como en `HKEY_LOCAL_MACHINE`. La clave **TWITaskbarGroupingMode** está disponible, por ejemplo, en HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Seamless Windows. [CVADHELP-19106]

### Instalación, desinstalación, actualización de versiones

- Cuando los clientes usan el servicio de personalización de aplicaciones, es posible que el instalador de Workspace se bloquee al validar el certificado. [RFWIN-21122]

## 2202

### Novedades

### Función Storebrowse para Workspace [Technical Preview]

A partir de esta versión, la aplicación Citrix Workspace para Windows permite usar Storebrowse para el autoservicio. Esto permite a los usuarios de Storebrowse acceder a las funciones de Cloud y Workspace.

> **Nota:**
>
> - Esta función permite usar Storebrowse solamente con Single Sign-On.
> - Los requisitos previos mencionados en Requisitos y compatibilidad del sistema deben estar disponibles para usar esta función.

Para obtener más información, consulte Storebrowse para Workspace.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción y compartan sus comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No se aconseja implementar compilaciones beta en entornos de producción.

### Citrix Enterprise Browser

Para ver las funciones o correcciones de errores de Citrix Enterprise Browser, consulte Novedades en la documentación de Citrix Enterprise Browser.

> **Nota:**
>
> Los requisitos del sistema de Citrix Workspace 2202 para Windows han cambiado de la siguiente manera:
>
> - La versión de .NET mínima requerida es 4.8.
> - La versión mínima de VCRedist requerida es 14.30.30704.0.

## Problemas resueltos

### Instalación, desinstalación, actualización de versiones

- Al actualizar la aplicación Citrix Workspace para Windows de la versión CU4 a la CU5 sin instalar el autoservicio, es posible que aparezca este mensaje:

  **Actualización de una versión no compatible**

  **Citrix Workspace desinstalará automáticamente la versión anterior y eliminará todos los parámetros, aunque podrá restaurarlos más adelante. De lo contrario, deberá eliminarlo todo manualmente. Haga clic en Aceptar para continuar.**

[CVADHELP-18790]

- Al intentar actualizar o iniciar una aplicación, aparece un mensaje de error que indica que **no se puede contactar con el almacén**. Este problema se produce cuando no se consigue obtener la descripción del acceso directo para aplicaciones suscritas concretas.

**Sus aplicaciones no están disponibles en este momento. Inténtelo de nuevo en unos minutos o póngase en contacto con el servicio de asistencia técnica con esta información: No se puede contactar con el almacén.**

[CVADHELP-18736]

### Sesión/Conexión

- Es posible que la tecla Imprimir pantalla no realice capturas de pantalla cuando la aplicación Citrix Workspace para Windows con la protección de aplicaciones habilitada se inicia en segundo plano. [RFWIN-25835]
- Al iniciar una aplicación publicada a través de un sitio de PNAgent en StoreFront mediante la aplicación Citrix Workspace para Windows, es posible que se produzca un error con este mensaje:

  **No se puede iniciar la aplicación. Póngase en contacto con el servicio de asistencia técnica.**

[CVADHELP-19209]

- Es posible que no se puedan iniciar sesiones desde grupos de entrega con una regla de directiva de acceso que especifique la dirección IP del cliente si el cliente tiene varias tarjetas NIC.

  ```
  Rule: Set-BrokerAccessPolicyRule -Name <rulename> -includedClientIPs <
  Client ip address>
  ```

[CVADHELP-18783]

- No se pueden crear accesos directos para aplicaciones publicadas a través de la aplicación Citrix Workspace sin los permisos adecuados. Como resultado, es posible que los iconos se descarguen en el perfil de usuario en cada actualización, lo que aumenta el tamaño de la memoria caché en los dispositivos de punto final y el consumo de CPU en el lado de StoreFront. [CVADHELP-18609]
- Después de configurar un almacén a través del objeto de directiva de grupo o el comando, es posible que no se actualice la interfaz de usuario de autoservicio abierta desde el área de notificaciones o desde el menú **Inicio**. Aparece el mensaje **No se puede contactar con el servidor**. [CVADHELP-19242]
- El escritorio virtual le pide que introduzca las credenciales aunque esté configurado PassThrough de dominio. Este problema se produce cuando inicia un escritorio virtual desde la aplicación Citrix Workspace. [RFWIN-26111]

- En la aplicación Citrix Workspace 2112.1, es posible que vea un uso elevado de la CPU en el dispositivo de punto final cuando la cámara web está encendida en videollamadas de Microsoft Teams optimizado. [HDX-37168]

## 2112.1

### Novedades

#### Función de detección de aplicaciones locales dentro de la aplicación Citrix Workspace

A partir de esta versión, los administradores pueden configurar la detección y la enumeración de aplicaciones instaladas localmente dentro de la aplicación Citrix Workspace. Puede configurar esta función mediante Global App Configuration Service. Para obtener más información sobre cómo configurar esta función, consulte Global App Configuration Service.
Esta función es ideal para dispositivos en modo quiosco y para aquellas aplicaciones que no se pueden virtualizar dentro de Citrix Workspace.

#### Continuidad del servicio

Durante una interrupción del servicio del proveedor de identidades para la autenticación del espacio de trabajo, es posible que los usuarios no puedan iniciar sesión en Citrix Workspace a través de la página de inicio de sesión de la aplicación Workspace.
El mensaje **¿Tiene problemas para iniciar sesión? Usar Workspace sin conexión** aparece en la parte superior de la pantalla de inicio de sesión de la aplicación Citrix Workspace.

Haga clic en **Usar Workspace sin conexión** para enumerar todas las aplicaciones y escritorios que tienen concesiones de conexión válidas almacenadas en el dispositivo cliente.

A partir de esta versión, el mensaje aparece después de esperar 40 segundos. Para obtener más información, consulte la sección Continuidad del servicio de la documentación de Citrix Workspace.

#### Experiencia en escritorios virtuales mejorada

Esta versión mejora la experiencia al cambiar el tamaño de los escritorios virtuales.

#### Seguridad de archivos ICA mejorada

En versiones anteriores, el archivo ICA se descargaba en el disco local al iniciar una sesión de aplicaciones y escritorios virtuales.

Con esta versión, ofrecemos una mayor seguridad en la forma en que la aplicación Citrix Workspace gestiona los archivos ICA durante el inicio de una sesión de aplicaciones y escritorios virtuales.

Ahora la aplicación Citrix Workspace le permite almacenar el archivo ICA en la memoria del sistema en lugar de hacerlo en el disco local. Esta función tiene como objetivo eliminar los ataques de superficie y cualquier malware que pueda utilizar incorrectamente el archivo ICA al almacenarlo localmente. Esta función también se puede aplicar a las sesiones de aplicaciones y escritorios virtuales que se inician en Workspace para Web.
Para obtener más información, consulte la sección Seguridad de archivos ICA mejorada.

#### Actualización de audio adaptable

El audio adaptable ahora funciona cuando se usa la entrega de audio UDP. Para obtener más información, consulte Audio adaptable.

#### Optimización de Microsoft Teams

> **Nota:**
>
> Estas funciones están disponibles solamente después de la implantación de una futura actualización de Microsoft Teams. Cuando Microsoft implante la actualización, consulte la hoja de ruta de Microsoft 365 o CTX253754 para obtener información sobre la actualización de la documentación y el anuncio.

- **Chat y reuniones multiventana para Microsoft Teams**

  Puede usar varias ventanas para reuniones y chats en Microsoft Teams con la optimización de HDX en Citrix Virtual Apps and Desktops 2112 o una versión posterior. Puede separar las conversaciones o las reuniones de varias maneras. Para obtener detalles sobre la función de ventana emergente, consulte Teams Pop-Out Windows for Chats and Meetings en el sitio de Microsoft Office 365.

  Si utiliza una versión anterior de la aplicación Citrix Workspace o Virtual Delivery Agent (VDA), recuerde que Microsoft retirará el código de las ventanas únicas en el futuro. Sin embargo, tendrá un mínimo de nueve meses después de que esta función esté generalmente disponible para actualizar VDA o la aplicación Citrix Workspace a una versión que admita varias ventanas (2112 o una versión posterior).

- **Uso compartido de aplicaciones**

  Antes no podía compartir aplicaciones mediante la función **Compartir pantalla** en Microsoft Teams al habilitar la directiva HDX 3D Pro en Citrix Studio.

  A partir de la aplicación Citrix Workspace 2112.1 para Windows y Citrix Virtual Apps and Desktops 2112, puede compartir aplicaciones mediante la función **Compartir pantalla** en Microsoft Teams cuando esta directiva está habilitada.

- **Dar control**

Puede usar el botón Dar control para otorgar el control de su pantalla compartida a otros usuarios que participan en la reunión. El otro participante puede seleccionar elementos y modificar la pantalla compartida mediante el teclado, el mouse y el portapapeles. Ahora los dos tienen el control de la pantalla compartida y usted puede recuperarlo cuando quiera.

- **Tomar el control**

  Durante las sesiones de uso compartido de pantalla, cualquier participante puede solicitar el control a través del botón Solicitar control. La persona que comparte la pantalla puede aprobar o rechazar la solicitud. Cuando tiene el control, puede controlar el teclado y el mouse en la pantalla compartida y liberar el control para dejar de compartir el control.

  **Limitación:**

  La opción **Solicitar el control** no está disponible durante llamadas entre un usuario optimizado y un usuario en el cliente de escritorio de Microsoft Teams nativo en el dispositivo de punto final. Como solución temporal, los usuarios pueden unirse a una reunión para obtener la opción **Solicitar el control**.

- **e911 dinámico**

  Con esta versión, la aplicación Citrix Workspace admite llamadas de emergencia dinámicas. Cuando se usa en los planes de llamadas de Microsoft, Operator Connect y enrutamiento directo, proporciona la capacidad de:

  - configurar y redirigir llamadas de emergencia
  - notificar al personal de seguridad

  La notificación se proporciona en función de la ubicación actual de la aplicación Citrix Workspace que se ejecuta en el dispositivo de punto final, en lugar del cliente de Microsoft Teams que se ejecuta en el VDA.
  La ley de Ray Baum exige que la ubicación transmitible de la persona que llama al 911 se transmita al Punto de Respuesta de Seguridad Pública (PSAP) correspondiente. A partir de la aplicación Citrix Workspace 2112.1 para Windows, la optimización para Microsoft Teams con HDX cumple con la ley de Ray Baum.

### Citrix Enterprise Browser

Esta versión de Enterprise Browser está basada en Chromium 95.

### Problemas resueltos

#### Instalación, desinstalación, actualización de versiones

Si instaló la aplicación Workspace con una versión anterior a 2109 como usuario y el administrador instala la versión 2109, aparece el mensaje de error **Entry point not found** si inicia sesión de nuevo en

el dispositivo como usuario. Si hace clic en **Aceptar**, el mensaje desaparece y la aplicación Workspace se actualiza a la versión 21.0.9. [RFWIN-25008]

### Iniciar sesión/autenticación

- Es posible que la autenticación de la aplicación Citrix Workspace falle tras la inicialización al intentar usar una tarjeta inteligente a través de Citrix Gateway. Si actualiza el proceso de autenticación después de 15 minutos, es posible que aparezca un mensaje de error 404 en un explorador integrado de Citrix Workspace. Esto hace que la aplicación se quede atascada en un bucle de autenticación hasta que cierre la aplicación y la abra de nuevo. [RFWIN-25006]
- Es posible que no se puedan agregar almacenes con autenticación por tarjeta y que aparezca este mensaje de error:
  **Este almacén no existe. Inténtelo de nuevo o póngase en contacto con asistencia.**
  [CVADHELP-18647]
- Al enumerar la aplicación a través de **Storebrowse**, se agrega un carácter nulo entre cada carácter en el archivo de enumeración. [CVADHELP-18773]

### Sesión/Conexión

- Es posible que la utilidad **Storebrowse** para enumerar recursos de la URL de Citrix Gateway falle cuando no se puede acceder a al menos uno de los Delivery Controllers configurados. [CVADHELP-15416]
- Al intentar abrir una aplicación si la opción **vPrefer** está habilitada y el límite de aplicaciones de una instancia por usuario está configurado, es posible que aparezca un error de conexión en Citrix Director. [CVADHELP-17372]
- Es posible que la aplicación Citrix Workspace sondee balizas externas para los almacenes internos solamente. Con esta corrección, las balizas externas no se sondean para los almacenes internos solamente o los almacenes que no tienen ninguna puerta de enlace asociada. [CVADHELP-18275]
- En la aplicación Citrix Workspace para Windows 2109 y versiones posteriores, es posible que la sesión de escritorio se desconecte al habilitar el modo de gráficos antiguo. [CVADHELP-18718]
- Al usar la protección de aplicaciones con la aplicación Citrix Workspace para Windows 2109 o una versión posterior, es posible que el rendimiento de la tarjeta gráfica sea deficiente. [CVADHELP-18831]
- Tras la actualización de versión automática de Microsoft Edge WebView2 Runtime, la aplicación Citrix Workspace para Windows muestra una pantalla vacía. [RFWIN-25295]
- La aplicación Citrix Workspace deja de funcionar. [RFWIN-25301]
- Controlar las fugas en componentes de la protección de aplicaciones provoca que algunos procesos fallen. [RFWIN-25358]

- Es posible que la función Desktop Lock de la aplicación Citrix Workspace falle si los almacenes de GPO de la configuración de Desktop Lock no están configurados. [RFWIN-25392]
- En Microsoft Teams, el uso compartido de la pantalla se detiene al cambiar el tamaño de la sesión. [HDX-31858]
- En el modo de varios monitores, aparece una pantalla vacía al desconectar la pantalla mientras comparte la pantalla en Microsoft Teams. [HDX-34733]
- Durante la sesión de pantalla compartida, el borde rojo que indica la pantalla compartida ocupa varias pantallas cuando Microsoft Teams se ejecuta en el modo integrado y en la configuración con varios monitores. [HDX-34978]
- Es posible que sufra errores en las llamadas durante llamadas P2P entre la aplicación Citrix Workspace para Mac 2109 y la aplicación Citrix Workspace para Windows 2109. [HDX-35223]
- Durante las videollamadas de Microsoft Teams, es posible que la cámara parpadee. [HDX-36345]
- Es posible que no se puedan iniciar sesiones al personalizar StoreFront y establecer el valor del campo en **ClientName** en el archivo default.ica. Para obtener más información, consulte el artículo CTX335725 de Citrix Knowledge Center. [CVADHELP-19033]

Para ver los problemas existentes en el producto, consulte la sección Problemas conocidos.

## 2109.1

### Novedades

#### Compatibilidad con Windows 11

Ahora la aplicación Citrix Workspace para Windows se admite en el sistema operativo Windows 11.

### Problemas resueltos

Si el administrador instaló extensiones externas en Google Chrome, Citrix Enterprise Browser se cierra de forma inesperada al abrirlo. [CTXBR-2135]

Para ver los problemas existentes en el producto, consulte la sección Problemas conocidos.

## 2109

### Novedades

#### Audio adaptable

Con el audio adaptable, no es necesario configurar las directivas de calidad de audio en los VDA. El audio adaptable optimiza los parámetros del entorno y sustituye los formatos de compresión de audio obsoletos para proporcionar una excelente experiencia de usuario.

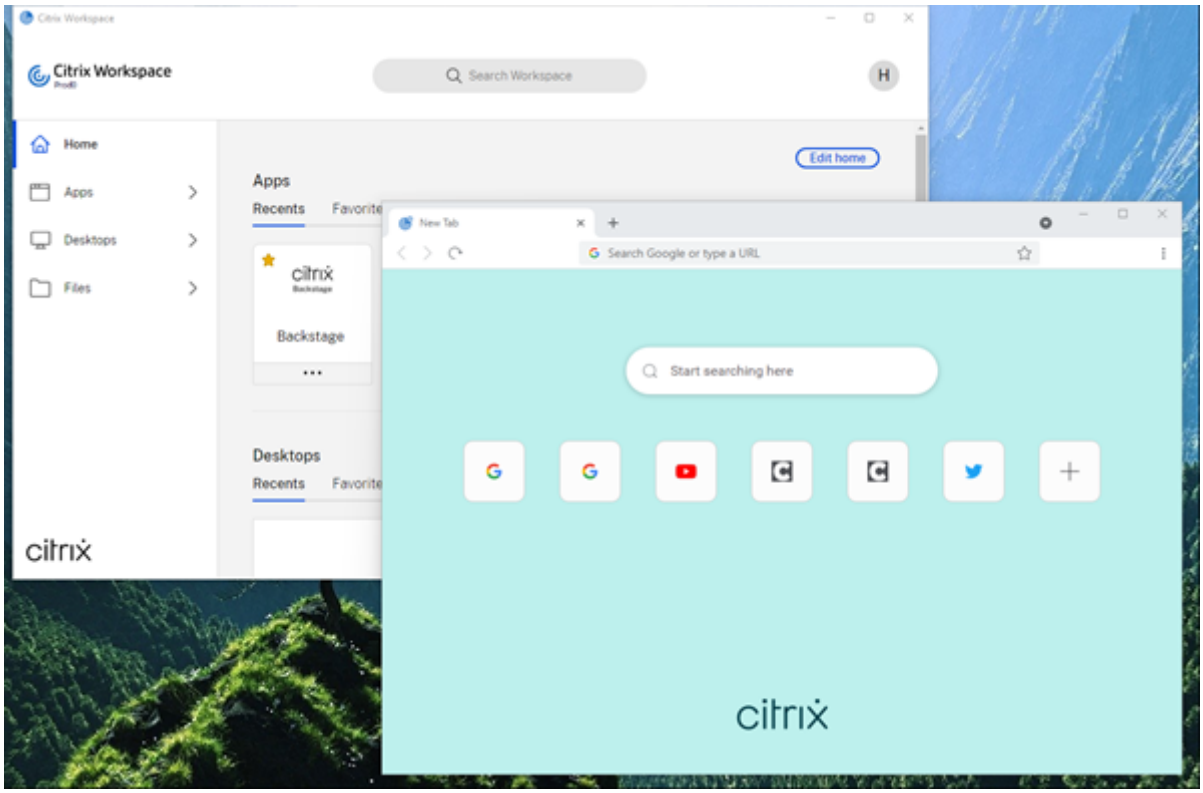
 

> **Nota:**
>
> Si se requiere la entrega de audio por UDP para la aplicación de audio en tiempo real, el audio adaptable debe estar inhabilitado en el VDA para que se pueda recurrir a la entrega de audio por UDP.

Para obtener más información, consulte Audio adaptable.

### Citrix Enterprise Browser

Citrix Enterprise Browser es un explorador web nativo que se ejecuta en la máquina cliente. Permite a los usuarios abrir aplicaciones web y SaaS desde la aplicación Citrix Workspace de forma segura.




Con un enfoque continuo en enriquecer la experiencia de usuario, el nuevo explorador ofrece una experiencia de usuario mejorada y más nativa con estas funciones:

- Acceso sin VPN a páginas web internas
- Compatibilidad con micrófonos y cámaras web
- Experiencia de navegación por fichas
- Vistas con varias ventanas
- Barra de direcciones (omnibox) modificable
- Marcadores
- Accesos directos en la página de la nueva ficha
- Parámetros personalizables

- Compatibilidad con la autenticación de proxy
- Análisis

Los administradores pueden habilitar Secure Private Access (antes, Secure Workspace Access) o directivas de protección de aplicaciones en diferentes combinaciones por dirección URL. Las funcionalidades incluyen la protección contra la captura de tecleo y contra las capturas de pantalla, descargas, impresión, restricciones del portapapeles y marcas de agua.

Para obtener más información, consulte Citrix Enterprise Browser.

#### Migración de URL de StoreFront a Workspace

A medida que su organización pase de almacenes locales de StoreFront a Workspace, los usuarios finales deberán agregar manualmente la nueva URL de su espacio de trabajo a la aplicación Workspace en sus dispositivos de punto final. Esta función permite a los administradores migrar a usuarios fácilmente de un almacén de StoreFront a un almacén de Workspace con una interacción mínima de los usuarios.

Para obtener más información sobre esta función, consulte Migración de URL de StoreFront a Workspace.

#### Compatibilidad con almacenes web personalizados

Con esta versión, puede acceder al almacén web personalizado de su organización desde la aplicación Citrix Workspace para Windows.

Para usar esta función, el administrador debe agregar el dominio o el almacén web personalizado a la lista de URL permitidas en Global App Configuration Service. Al agregarlos, puede proporcionar la URL del almacén web personalizado en la pantalla **Agregar cuenta** de la aplicación Citrix Workspace. El almacén web personalizado se abre en la ventana de la aplicación Workspace nativa.

Para obtener más información sobre la configuración de almacenes web personalizados, consulte Almacenes web personalizados.

#### Compatibilidad con la autenticación con claves de seguridad FIDO2 y Windows Hello

Con esta versión, puede autenticarse en Citrix Workspace mediante claves de seguridad FIDO2 y Windows Hello.

Para obtener más información, consulte Otras maneras de autenticarse en Citrix Workspace.

#### Single Sign-On (SSO) en la aplicación Citrix Workspace desde máquinas unidas a Microsoft Azure Active Directory (AAD) con AAD como proveedor de identidades

Con esta versión, puede iniciar sesión mediante SSO en la aplicación Citrix Workspace desde máquinas unidas a Azure Active Directory (AAD) con AAD como el proveedor de identidades.

Para obtener más información, consulte Otras maneras de autenticarse en Citrix Workspace.

#### Compatibilidad del Acceso condicional con Azure Active Directory

Con esta versión, los administradores de Workspace pueden configurar y aplicar directivas de acceso condicional de Azure Active Directory para usuarios que se autentican en la aplicación Citrix Workspace.

Para obtener más información, consulte Compatibilidad con el acceso condicional con Azure AD.

#### Compatibilidad con la continuidad del servicio

Esta versión ofrece continuidad del servicio con extensiones web de Citrix Workspace. Puede usar extensiones web de Workspace para Google Chrome o Microsoft Edge con la aplicación Workspace para Windows 2109. Estas extensiones están disponibles en el Chrome Web Store de Google y en el sitio web de complementos de Microsoft Edge.
La aplicación Workspace se comunica con la extensión web de Citrix Workspace mediante el protocolo del host de mensajería nativa para extensiones de explorador. Juntos, la aplicación Workspace y la extensión web de Workspace utilizan las concesiones de conexión de Workspace para proporcionar a los usuarios del explorador acceso a sus aplicaciones y escritorios durante desconexiones.
Para obtener más información, consulte Continuidad del servicio.

#### Mejoras de Microsoft Teams

Estas funciones están disponibles solamente después de la implantación de una futura actualización de Microsoft Teams.

Cuando Microsoft implante la actualización, consulte CTX253754 para obtener información sobre la actualización de la documentación y el anuncio.

- **Compatibilidad con WebRTC**: Esta versión admite WebRTC 1.0 para ofrecer una mejor experiencia en videoconferencias junto en la vista de galería.
- **Mejora del uso compartido de la pantalla**: Puede compartir aplicaciones individuales, ventanas o la pantalla completa mediante la función de uso compartido de la pantalla en Microsoft Teams. Citrix Virtual Delivery Agent 2109 es un requisito previo para esta función.
- **Compatibilidad con la protección de aplicaciones**: Ahora, cuando la protección de aplicaciones está habilitada, puede compartir contenido a través de Microsoft Teams con la optimización de HDX.
  Con esta función, puede compartir la ventana de aplicaciones que se ejecutan en el escritorio virtual. Citrix Virtual Delivery Agent 2109 es un requisito previo para esta función.

> **Note:**
>
> Full monitor or desktop sharing is disabled when App Protection is enabled for the delivery group.

- **Subtítulos en directo**: Esta versión ofrece la transcripción en tiempo real de lo que dicen los ponentes cuando Subtítulos en directo esté habilitado en Microsoft Teams.

#### Optimización de Microsoft Teams

La versión de Citrix Workspace 2109 para Windows permite llamadas de audio y vídeo, llamadas de conferencia y el uso compartido de la pantalla entre dos usuarios en Microsoft Teams optimizado en aplicaciones alojadas en máquinas virtuales.

#### Compatibilidad con teclados Bloomberg 5

Esta versión permite usar teclados Bloomberg 5. Para usar el teclado Bloomberg 5, debe configurar el Editor del Registro. Para obtener más información sobre cómo configurar el teclado, consulte la sección Configurar el teclado Bloomberg 5 en Teclados Bloomberg.

### Problemas resueltos

#### Ventanas integradas

Es posible que algunas aplicaciones de terceros permanezcan en primer plano y dejen otras aplicaciones iniciadas en segundo plano. [CVADHELP-16897]

#### Interfaz de usuario

Al usar la aplicación Citrix Workspace para Windows, es posible que los accesos directos del menú Inicio no se actualicen automáticamente. El problema ocurre al agregar una nueva aplicación o al realizar un cambio en el back-end. [CVADHELP-17122]

#### Problemas en el dispositivo cliente

Al usar la aplicación Citrix Workspace, es posible que los dispositivos conectados con puertos COM superiores a 9 no se asignen en la sesión. [CVADHELP-17734]

#### Sesión/Conexión

- Al actualizar la versión de la aplicación Citrix Workspace para Windows a la versión 2106, es posible que no se puedan iniciar aplicaciones o escritorios con un servidor proxy y que aparezca este mensaje de error:

**No se puede conectar con el servidor. Notifique al administrador del sistema el siguiente error: No hay ningún servidor de Citrix XenApp configurado en la dirección especificada (Error de socket 10060)** [CVADHELP-18137]

- Al intentar redirigir una cámara web mediante la aplicación Citrix Workspace para Windows instalada en un VDA, es posible que la cámara falle. [HDX-28691]
- Si comparte su pantalla en Microsoft Teams con la optimización de HDX en una configuración de varios monitores, el selector del uso compartido de la pantalla no captura monitores individuales. Este problema se produce cuando el escritorio virtual no utiliza la barra de herramientas de Desktop Viewer o utiliza Desktop Lock. En lugar de un monitor individual, todos los monitores se condensan en una sola imagen compuesta. Es posible que vea este problema en la aplicación Citrix Workspace para Windows 2106 o en una versión posterior.
  En esta versión se inhabilita la funcionalidad del uso compartido de la pantalla con varios monitores:
- Si Desktop Viewer está inhabilitado en StoreFront o en el archivo ICA
- O si el Desktop Lock se está usando Solo se puede compartir el monitor principal. [HDX-34200]

Para ver los problemas existentes en el producto, consulte la sección Problemas conocidos.

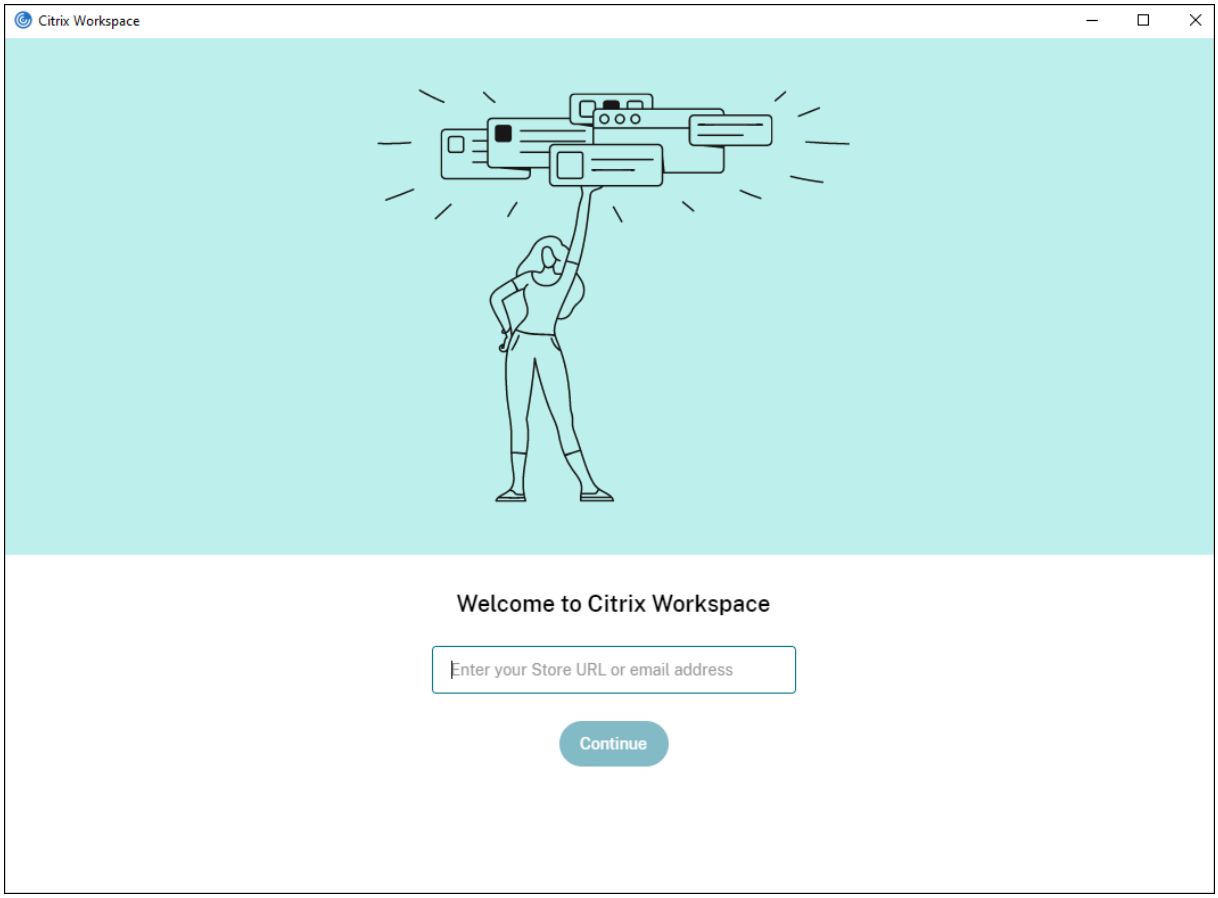
### 2108

#### Novedades

#### Pantalla para agregar cuentas rediseñada

Esta versión presenta una pantalla Agregar cuenta rediseñada.




**Tiempo de espera por inactividad en sesiones de Citrix Workspace**

Los administradores pueden configurar el valor del tiempo de espera por inactividad. El valor del tiempo de espera por inactividad especifica el tiempo de inactividad permitido antes de que se cierre automáticamente la sesión de usuario de Citrix Workspace. Si no hay actividad en el mouse, en el teclado ni en comandos táctiles durante el intervalo de tiempo especificado, la sesión de la aplicación Citrix Workspace se cierra automáticamente. El tiempo de espera por inactividad no afecta a las sesiones de aplicaciones y escritorios virtuales ni a almacenes de Citrix StoreFront.

Para obtener más información, consulte Tiempo de espera por inactividad en sesiones de Workspace.

> **Nota:**
>
> Los administradores pueden configurar el tiempo de espera por inactividad solamente para sesiones de Workspace (nube).

**Función de almacenes web personalizados [Technical Preview]**

Con esta versión, puede acceder al almacén web personalizado de su organización desde la aplicación Citrix Workspace para Windows. Para usar esta función, el administrador debe agregar el dominio o

el almacén web personalizado a la lista de URL permitidas en Global App Configuration Service. Al agregarlos, puede proporcionar la URL del almacén web personalizado en la pantalla **Agregar cuenta** de la aplicación Citrix Workspace. El almacén web personalizado se abre en la ventana de la aplicación Workspace nativa.

Para obtener información sobre la configuración de almacenes web personalizados, consulte Almacenes web personalizados.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción y compartan sus comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No se aconseja implementar compilaciones beta en entornos de producción.

#### Migración de URL de StoreFront a Workspace [Technical Preview]

Cuando su organización pase de almacenes locales de StoreFront a Workspace, los usuarios finales deberán agregar manualmente la nueva URL de su espacio de trabajo a la aplicación Workspace en sus dispositivos de punto final. Esta función permite a los administradores migrar a usuarios fácilmente de un almacén de StoreFront a un almacén de Workspace con una interacción mínima de los usuarios.

Para obtener más información sobre esta función, consulte Migración de URL de StoreFront a Workspace [Technical Preview]

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción y compartan sus comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No se aconseja implementar compilaciones beta en entornos de producción.

### Problemas resueltos

#### Inicio de sesión/Autenticación

Si se agota el tiempo de espera en una sesión de Citrix Gateway, es posible que Citrix Workspace no solicite la autenticación al iniciar una aplicación. [RFWIN-23829]

Para ver los problemas existentes en el producto, consulte la sección Problemas conocidos.

## 2107

### Novedades

#### Mejora de EPA

A partir de esta versión, la aplicación Citrix Workspace puede descargar e instalar el plug-in de EPA en implementaciones de Workspace. Una vez completada la instalación, Advanced Endpoint Analysis (EPA) analiza el dispositivo para buscar requisitos de seguridad de dispositivos de punto final configurados en Citrix Gateway. Al completarse el análisis, aparece la ventana de inicio de sesión de la aplicación Citrix Workspace.

> **Nota:**
>
> Esta función solo está operativa si configuró la autenticación nFactor en su entorno.

Para obtener más información sobre el análisis de EPA, consulte Advanced Endpoint Analysis scans.

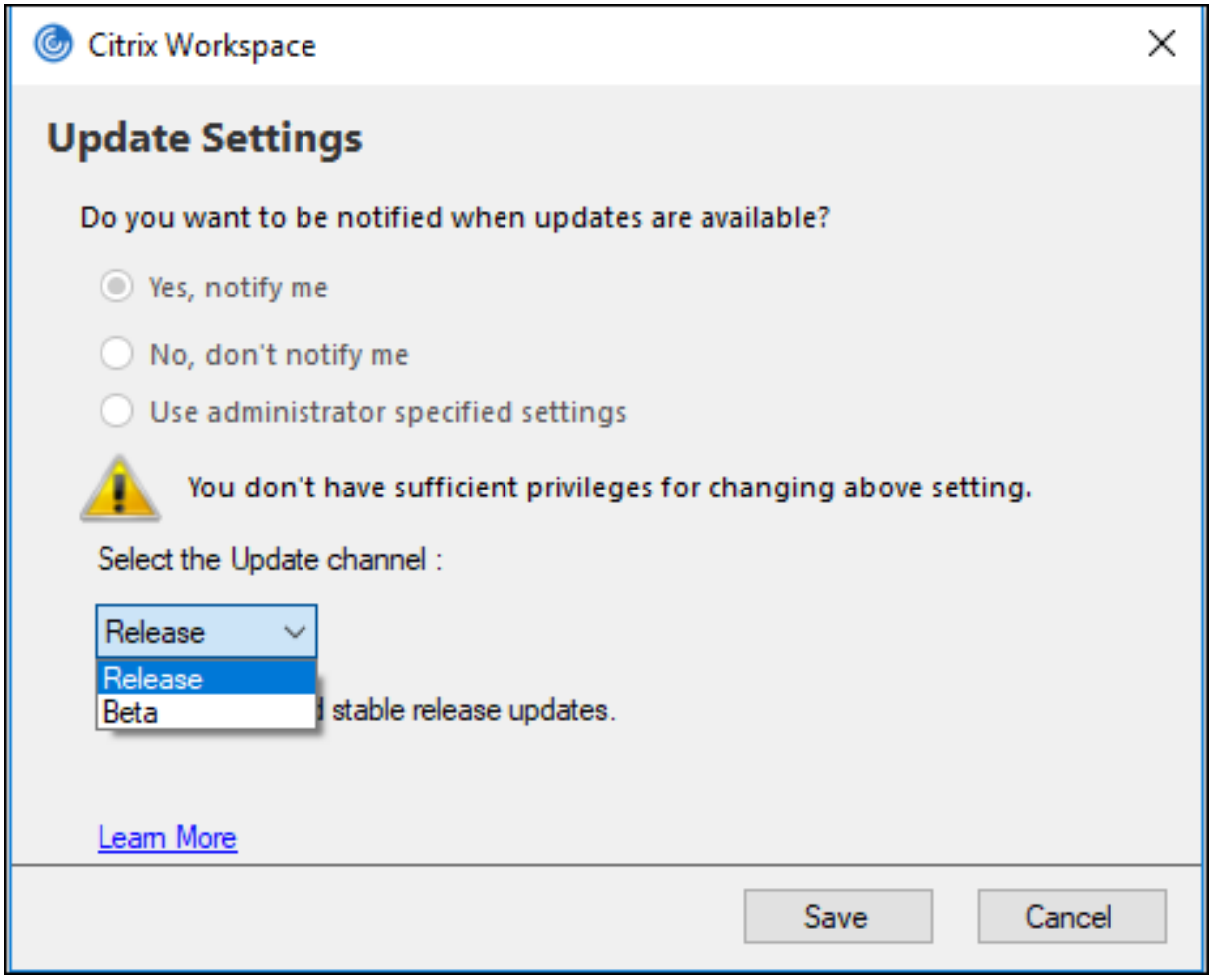
#### Programa Beta de la aplicación Citrix Workspace

A partir de esta versión, podrá actualizar automáticamente las instalaciones existentes de Citrix Workspace a las compilaciones Beta más recientes y probarlas. Las compilaciones Beta son versiones de acceso anticipado publicadas antes de la disponibilidad general de actualizaciones públicas, estables y totalmente funcionales. Recibirá una notificación de actualización cuando la Citrix Workspace se haya configurado para obtener actualizaciones automáticas.

Para actualizar su versión a una compilación Beta, seleccione el **canal Beta** en el menú desplegable de la ventana **Parámetros de actualización**:

- **Público:** Actualización pública, estable y totalmente funcional.
- **Beta:** Versión de acceso anticipado para probar y notificar problemas fácilmente antes de su disponibilidad general.




> **Nota:**
>
> Las compilaciones beta están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción y para compartir comentarios. Citrix no acepta casos de asistencia de compilaciones beta, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No se aconseja implementar compilaciones beta en entornos de producción.

Para obtener más información sobre la instalación de canales de actualización automática, consulte Instalar el programa Beta de la aplicación Citrix Workspace.

#### Compatibilidad con los siguientes mecanismos de autenticación [Technical Preview]

A partir de esta versión, puede autenticarse en la aplicación Citrix Workspace mediante los siguientes mecanismos:

- Autenticación con claves de seguridad FIDO2 y Windows Hello
- Single Sign-On (SSO) en la aplicación Citrix Workspace desde máquinas unidas a Microsoft Azure Active Directory (AAD) con AAD como proveedor de identidades

### Requisitos del sistema

Versión 92 de Microsoft Edge WebView2 Runtime o una posterior.

> **Nota:**
>
> A partir de la versión 2107, el instalador de Microsoft Edge WebView2 Runtime se empaqueta con el instalador de la aplicación Citrix Workspace. Durante la instalación de la aplicación Workspace, el instalador comprueba si Microsoft Edge WebView2 Runtime está presente en el sistema y, si no lo encuentra, lo instala.
>
> Si intenta instalar la aplicación Citrix Workspace como un usuario que es administrador y Microsoft Edge WebView2 Runtime no está presente, la instalación se detiene con este mensaje:
>
> ```
> You must be logged on as an administrator to install the following
> prerequisite package(s):
> ```
>
> ```
> Edge Webview2 Runtime
> ```
>
> Esta función solo está disponible en implementaciones de Workspace (Cloud).

### Habilitar los mecanismos de autenticación

Para habilitar los mecanismos de autenticación, los administradores deben seguir estos pasos:

1. Abra el Editor del Registro.
2. Vaya a esta ruta del Registro:
   - Como administrador:
     - Para sistemas operativos Windows de 64 bits: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle`
     - Para sistemas operativos Windows de 32 bits: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`
   - Como no administrador:
     - Para sistemas operativos de 64 o 32 bits: `\HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle`
3. Cree un valor del Registro con estos atributos:

   **Nombre de la clave del Registro:** EdgeChromiumEnabled

   **Tipo:** Valor de la cadena

   **Valor:** True
4. Reinicie la aplicación Citrix Workspace para que los cambios surtan efecto.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las usen en sus entornos de producción limitados o en entornos que no son de producción y compartan sus comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia.

#### Compatibilidad con el acceso condicional con Azure AD [Technical Preview]

Con esta versión, puede autenticarse con el acceso condicional si el administrador configura las directivas pertinentes.

#### Requisitos del sistema

Versión 92 de Microsoft Edge WebView2 Runtime o una posterior.

> **Nota:**
>
> A partir de la versión 2107, el instalador de Microsoft Edge WebView2 Runtime se empaqueta con el instalador de la aplicación Citrix Workspace. Durante la instalación de la aplicación Workspace, el instalador comprueba si Microsoft Edge WebView2 Runtime está presente en el sistema y, si no lo encuentra, lo instala.

#### Habilitar la autenticación mediante el acceso condicional

Para habilitar la autenticación mediante el acceso condicional con Azure AD, los administradores deben seguir estos pasos:

1. Abra el Editor del Registro.
2. Vaya a esta ruta del Registro:
   - Para sistemas operativos Windows de 64 bits: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle`
   - Para sistemas operativos Windows de 32 bits: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`
3. Cree un valor del Registro con estos atributos:

   **Nombre de la clave del Registro:** EdgeChromiumEnabled

   **Tipo:** Valor de la cadena

   **Valor:** True
4. Reinicie la aplicación Citrix Workspace para que los cambios surtan efecto.

### Función de detección de aplicaciones locales dentro de la aplicación Workspace [Technical Preview]

A partir de la versión 2107, los administradores pueden configurar la detección y la enumeración de aplicaciones instaladas localmente dentro de la aplicación Citrix Workspace. Puede configurar esta función mediante Global App Configuration Service. Para obtener más información sobre cómo configurar esta función, consulte Global App Configuration Service.

Esta función es ideal para dispositivos en modo quiosco y para las aplicaciones que no se pueden virtualizar dentro de Citrix Workspace.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las usen en sus entornos de producción limitados o en entornos que no son de producción y compartan sus comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia.

## Problemas resueltos

### Teclado

Con la protección de aplicaciones instalada, es posible que las entradas de teclado no sean compatibles con algunos portátiles de la serie G5 de HP. [RFWIN-24103]

### Sesión/Conexión

- Con la función de arrastrar y colocar habilitada, es posible que no se pueda cambiar el tamaño de una aplicación publicada. [CVADHELP-17089]
- Al configurar el cliente y el VDA con parámetros de proxy de red, es posible que la redirección de contenido del explorador web falle en el explorador Chrome. [CVADHELP-17430]
- Con Single Sign-On, al iniciar sesión con una credencial UPN y, a continuación, cambiar la contraseña en el dispositivo de punto final, es posible que aparezca este mensaje de error después de intentar iniciar una sesión:

  **El nombre de usuario o la contraseña no son correctos. Reintentar.** [CVADHELP-17620]
- Al iniciar una videollamada durante una reunión de Microsoft Teams, es posible que Desktop Viewer deje de responder. [HDX-32435]

Para ver los problemas existentes en el producto, consulte la sección Problemas conocidos.

## 2106

### Novedades

#### Global App Config Service

El nuevo Citrix Global App Configuration Service para Citrix Workspace ofrece a los administradores de Citrix la capacidad de entregar direcciones URL de servicio de Workspace y parámetros de la aplicación Workspace a través de un servicio administrado de forma centralizada.

Para obtener más información, consulte la documentación de Global App Configuration Service.

#### Opción para inhabilitar el almacenamiento de tokens de autenticación mediante Global App Config Service

Ahora la aplicación Citrix Workspace ofrece una opción adicional para inhabilitar el almacenamiento de tokens de autenticación en el disco local. Junto con la configuración existente de objetos de directiva de grupo (GPO), también puede inhabilitar el almacenamiento de tokens de autenticación en el disco local mediante Global App Configuration Service.

En Global App Configuration Service, establezca el atributo `Store Authentication Tokens` en `False`.

Para obtener más información, consulte la documentación de Global App Configuration Service.

#### Continuidad del servicio

La continuidad del servicio elimina o minimiza la dependencia de la disponibilidad de los componentes involucrados en el proceso de conexión. Los usuarios pueden iniciar sus aplicaciones y escritorios virtuales, independientemente del estado de los servicios en la nube.

Para obtener más información, consulte la sección Continuidad del servicio de la documentación de Citrix Workspace.

#### Mejoras de Microsoft Teams

Cuando Desktop Viewer se halla en modo de pantalla completa, el usuario puede seleccionar una de todas las pantallas que cubren Desktop Viewer para compartirla. En el modo de ventana, el usuario puede compartir la ventana de **Desktop Viewer**. En el modo integrado, el usuario puede seleccionar una de todas las pantallas para compartirla. Cuando Desktop Viewer cambia el modo de ventana (maximizada, restaurada o minimizada), la pantalla compartida se detiene.

#### Función de URL bidireccionales con exploradores web basados en Chromium

La redirección bidireccional de contenido permite configurar direcciones URL para redirigir contenido del cliente al servidor y del servidor al cliente. Puede configurarla mediante directivas en el servidor y en el cliente.

Mediante la plantilla administrativa de objetos de directiva de grupo (GPO), puede establecer directivas de servidor en el Delivery Controller y directivas de cliente en la aplicación Citrix Workspace.

Esta versión ofrece la redirección bidireccional de URL para Google Chrome y Microsoft Edge.

**Requisitos previos:**

- Citrix Virtual Apps and Desktops 2106 o una versión posterior.
- Versión 5.0 de la extensión de redirección del explorador web.

Para registrar el explorador web Google Chrome en la redirección bidireccional de URL, ejecute este comando desde la carpeta de instalación de la aplicación Citrix Workspace:

```
%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regChrome /
    verbose
```

Para cancelar el registro del explorador web Google Chrome de la redirección bidireccional de URL, ejecute este comando desde la carpeta de instalación de la aplicación Citrix Workspace:

```
%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe  /unregChrome /
    verbose
```

Para obtener información sobre cómo configurar la redirección de URL en la aplicación Citrix Workspace, consulte Redirección de contenido bidireccional.

Para obtener más información sobre la redirección de contenido del explorador web, consulte Redirección de contenido de explorador web en la documentación de Citrix Virtual Apps and Desktops.

#### Seguridad de archivos ICA mejorada [Technical Preview]

En versiones anteriores, el archivo ICA se descargaba en el disco local al iniciar una sesión de aplicaciones y escritorios virtuales.

Con esta versión, ofrecemos una mayor seguridad en la forma en que la aplicación Citrix Workspace gestiona los archivos ICA durante el inicio de una sesión de aplicaciones y escritorios virtuales.

Ahora la aplicación Citrix Workspace le permite almacenar el archivo ICA en la memoria del sistema en lugar de hacerlo en el disco local. Esta función tiene como objetivo eliminar los ataques de superficie y cualquier malware que pueda utilizar incorrectamente el archivo ICA al almacenarlo localmente. Esta función también se puede aplicar a las sesiones de aplicaciones y escritorios virtuales que se inician en Workspace para Web.

Para obtener más información, consulte la sección Seguridad de archivos ICA mejorada.

Para enviar comentarios sobre esta función, utilice el formulario de Podio.

### Problemas resueltos

#### Sesión/Conexión

- Es posible que se produzca un error al intentar imprimir un archivo con Citrix PDF Printer al usar Google Chrome, Mozilla Firefox o Microsoft Internet Explorer como visores de PDF predeterminados. [CVADHELP-16662]
- Después de actualizar la aplicación Citrix Workspace para Windows a la versión 1912 LTSR CU1 o CU2, es posible que se produzca un error en la fiabilidad de las sesiones. El problema se produce cuando el protocolo Enlightened Data Transport (EDT) está establecido y la conexión pasa por Citrix Gateway. [CVADHELP-16694]
- Es posible que no se puedan iniciar aplicaciones mediante la aplicación Citrix Workspace para Windows cuando la VPN se conecta o se desconecta. [CVADHELP-16714]
- En casos de doble salto, es posible que los nombres de cliente de los dispositivos de punto final no pasen al Delivery Controller o a Director. El problema se produce con la versión 2003 de VDA y versiones posteriores. [CVADHELP-16783]
- Es posible que no surta efecto establecer el valor `CurrentAccount` en `AllAccount` el Registro `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle`. El problema se produce cuando hay al menos una cuenta de almacén presente. [CVADHELP-17229]
- Es posible que no se pueda iniciar sesión en la aplicación Citrix Workspace para Windows cuando el nombre de usuario contiene caracteres con diéresis. [CVADHELP-17267]
- Es posible que no se puedan descargar archivos alojados en una red local. [CVADHELP-17337]
- Durante una conferencia telefónica, cuando se utiliza Microsoft Teams en modo optimizado HDX, es posible que la parte del vídeo de las llamadas entrantes parpadee. [CVADHELP-17398]
- Es posible que no se puedan descargar archivos mediante las microaplicaciones. [CVADHELP-17438]

#### Interfaz de usuario

- Al usar el Editor de métodos de entrada (IME) chino o japonés para escribir en un cuadro de texto, es posible que el texto aparezca fuera del cuadro de texto en la esquina superior izquierda de la pantalla. [CVADHELP-15614]
- Al intentar iniciar una aplicación desde un acceso directo, es posible que el icono del acceso directo parpadee en algunos escritorios. Este problema se produce después de actualizar la versión 4.9.6 de Citrix Receiver para Windows a la aplicación Citrix Workspace. [CVADHELP-16967]
- Es posible que no se pueda ejecutar la prueba de baliza en `ping.citrix.com`. [RFWIN-22672]
- Es posible que la continuidad del servicio no sea compatible con todos los usuarios que tienen nombres de usuario Unicode en sus dispositivos Windows y nombres de usuario ASCII en su

cuenta de Citrix Workspace. Si el nombre de usuario Unicode contiene caracteres cirílicos o asiáticos orientales, no se inician las concesiones de conexión de Workspace para estos usuarios. [RFWIN-23040, RFWIN-23046]

Para ver los problemas existentes en el producto, consulte la sección Problemas conocidos.

## 2105

### Novedades

#### Compatibilidad con direcciones URL personalizadas a través de redirecciones 301

Ahora la aplicación Citrix Workspace le permite agregar direcciones URL que redirigen a Citrix Workspace desde StoreFront o Citrix Gateway a través de redirecciones HTTP 301.

Si migra de StoreFront a Citrix Workspace, puede redirigir la URL de StoreFront a una URL de Citrix Workspace mediante una redirección HTTP 301. Como resultado, al agregar una URL antigua de StoreFront, se le redirige automáticamente a Citrix Workspace.

**Ejemplo de una redirección:**

La URL de StoreFront `https://< Citrix Storefront url>/Citrix/Roaming/Accounts` se puede redirigir a una URL de Citrix Workspace: `https://<Citrix Workspace url>/Citrix/Roaming/Accounts`.

#### Mejora para Microsoft Teams

- Ahora puede configurar una interfaz de red preferida para el tráfico multimedia.

  Vaya a `\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream` y cree una clave llamada `NetworkPreference`(REG_DWORD).

  Seleccione uno de estos valores según corresponda:

  - 1: Ethernet
  - 2: Wi-Fi
  - 3: Móvil
  - 5: Bucle invertido
  - 6: Cualquiera

  De forma predeterminada y si no se establece ningún valor, el motor de medios WebRTC elige la mejor ruta disponible.

- Ahora puede inhabilitar el módulo del dispositivo de audio 2 (ADM2) para que el módulo de dispositivo de audio (ADM) heredado se utilice para micrófonos de cuatro canales. Inhabilitar ADM2 ayuda a resolver problemas relacionados con los micrófonos en las llamadas.

Para inhabilitar ADM2, vaya a `\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`, cree una clave denominada `DisableADM2` (REG_DWORD) y establezca el valor en `1`.

Para ver los problemas existentes en el producto, consulte la sección Problemas conocidos.

### Problemas resueltos

#### Sesión/Conexión

- Al utilizar la aplicación Citrix Workspace para Windows, es posible que los recursos protegidos de aplicaciones no se inicien y permanezcan atascados en la pantalla de conexión. El problema se produce con la aplicación Citrix Workspace instalada en sistemas operativos de servidor, como Windows Server 2019. [RFWIN-22120]
- Es posible que no se puedan ejecutar comandos en Git bash. El problema se produce con la aplicación Citrix Workspace que tiene habilitada la función de protección de aplicaciones. [RFWIN-22187]
- Después de instalar la versión más reciente de la aplicación Citrix Workspace, es posible que aparezca una solicitud para actualizar la versión al iniciar sesión en StoreFront. [RFWIN-22419]
- Es posible que no se pueda salir de la aplicación Citrix Workspace. El problema se produce cuando la solicitud de credenciales de usuario aparece repetidamente. [RFWIN-22491]
- Después de crear un acceso directo de escritorio para una aplicación y reiniciar el dispositivo cliente, es posible que no se pueda iniciar la aplicación desde el acceso directo la primera vez. El problema se produce cuando no se especifica `storedescription` al instalar la aplicación Citrix Workspace mediante la interfaz de línea de comandos. [RFWIN-22510]
- Al descargar un archivo de Citrix Files, es posible que no se lean bien nombres de archivo que no estén en inglés. [RFWIN-22516]
- Con la protección de pila reforzada por hardware habilitada y las funciones HSP o CET disponibles, es posible que las aplicaciones se cierren de forma inesperada en procesadores Intel Core de 11.ª generación y procesadores AMD Ryzen de la serie 5000. [RFWIN-22592]
- Si la directiva Transporte adaptable HDX está establecida en Preferido y Detección de MTU en EDT está habilitada, al intentar iniciar aplicaciones o escritorios, es posible que aparezca una pantalla gris o negra con un mensaje de advertencia. [RFWIN-22697]
- Es posible que la aplicación Citrix Workspace para Windows no pueda enumerar aplicaciones y se quede atascada en una pantalla gris. Es un problema específico de la tarjeta gráfica Intel Iris Xe. [RFWIN-22952]
- Durante las videollamadas de dos usuarios de Microsoft Teams, es posible que el proceso HdxRtcEngine.exe deje de responder. El problema se produce en configuraciones de varios monitores con diferentes resoluciones de pantalla. [HDX-28616]
- Al unirse a una reunión de Microsoft Teams desde Outlook, es posible que el vídeo entrante no funcione. El problema se produce al unirse a la reunión sin iniciar Microsoft Teams. [HDX-29558]
- Durante las reuniones de Microsoft Teams, al pasar el puntero del mouse sobre el vídeo, es posi-

ble que el vídeo parpadee. [HDX-29668]

#### Excepciones del sistema

- Es posible que el proceso `Wfica32.exe` se cierre de forma inesperada por un error en el módulo gfxrender.dll. [RFWIN-22446]

#### Problemas de seguridad

- En una instancia instalada por el administrador de la aplicación Citrix Workspace, es posible que los usuarios con privilegios no administrativos puedan aumentar el nivel de privilegios. Para obtener más información, consulte el artículo CTX307794 de Citrix Knowledge Center.

Para ver los problemas existentes en el producto, consulte la sección Problemas conocidos.

### 2103.1

#### Novedades

#### Mejora en la configuración de la distribución del teclado

Ahora la configuración de la distribución del teclado incluye la opción **No sincronizar**. La opción está disponible tanto para la directiva de objeto de directiva de grupo (GPO) como para las configuraciones de la GUI.

Al seleccionar la opción **No sincronizar**, la distribución del teclado del servidor se utiliza en la sesión y la distribución del teclado del cliente no se sincroniza con la distribución del teclado del servidor.

Para obtener más información, consulte Barra de idioma y distribución del teclado.

#### Opción para inhabilitar el almacenamiento de tokens de autenticación

Los tokens de autenticación se cifran y se almacenan en el disco local para que no tenga que volver a escribir sus credenciales al reiniciar el sistema o la sesión.

La aplicación Citrix Workspace presenta una opción para inhabilitar el almacenamiento de tokens de autenticación en el disco local. Para mejorar la seguridad, ahora proporcionamos una directiva de objeto de directiva de grupo (GPO) para configurar el almacenamiento de tokens de autenticación.

> **Nota:**
>
> Esta configuración solo se puede aplicar en implementaciones en la nube.

Para obtener más información, consulte Tokens de autenticación.

### Mejoras de Microsoft Teams

- Ahora el códec de vídeo VP9 está inhabilitado de forma predeterminada.
- Mejora en la eliminación de eco, el control automático de ganancias y configuraciones de supresión de ruido: Si Microsoft Teams configura estas opciones, la instancia de Microsoft Teams redirigida por Citrix respeta los valores tal y como están configurados. De lo contrario, estas opciones se establecen en **True** de forma predeterminada.
- Ahora `DirectWShow` es el generador predeterminado.

  **Para cambiar el generador predeterminado, haga esto:**

  - Abra el Editor del Registro.
  - Vaya a esta ubicación de clave: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream` .
  - Actualice este valor: `"UseDirectShowRendererAsPrimary"=dword:00000000`

    Otros valores posibles:

    * 0: Media Foundation
    * 1: DirectShow (predeterminado)
  - Vuelva a iniciar la aplicación Citrix Workspace.

### Problemas resueltos

### Inicio de sesión/Autenticación

- Incluso después de habilitar las directivas Mantener mi sesión conectada y No volver a preguntar durante 60 días, es posible que la autenticación de varios factores de Microsoft Azure aún solicite la autenticación.

  > **Nota:**
  >
  > Recomendamos que los usuarios salgan de los almacenes en lugar de cerrar la sesión de los almacenes. Si los usuarios cierran la sesión de los almacenes mediante la autenticación de WebView, es posible que se les pida la autenticación de nuevo porque las cookies de Internet Explorer se borran en casos así. De forma predeterminada, la corrección está habilitada (se almacenan las cookies). Puede inhabilitar la corrección mediante la opción GPO. Si inhabilita la corrección, las cookies no se almacenan y se borran al cerrar la sesión.

  [CVADHELP-14814]
- En dispositivos unidos a Azure Active Directory (AD), cuando la aplicación Citrix Workspace intenta acceder a un almacén y, a continuación, pasa por las credenciales de inicio de sesión del dispositivo de punto final, es posible que no pueda autorizar el inicio de sesión. Además, no hay ninguna opción para iniciar sesión con otra cuenta de usuario. [CVADHELP-14844]

### Problemas de seguridad

- Esta corrección mejora la seguridad en un componente subyacente. [RFWIN-20912]

### Sesión/Conexión

- Al iniciar un escritorio publicado a través de una aplicación Citrix Workspace para Windows nativa, la aplicación Citrix Workspace nativa se ejecuta automáticamente en primer plano dentro del escritorio. El problema se produce cuando la función Acceso a aplicaciones locales está habilitada. [CVADHELP-15654]
- En situaciones en las que los servidores proxy no usan el puerto 8080, es posible que la aplicación Citrix Workspace no se pueda conectar a aplicaciones y escritorios publicados. El problema se produce cuando la aplicación Citrix Workspace para Windows no consigue usar el puerto del proxy y, en su lugar, usa el puerto 8080 predeterminado. [CVADHELP-15977]
- Es posible que la aplicación Citrix Workspace para Windows ignore los parámetros del tipo de proxy. El problema se produce en versiones no inglesas del sistema operativo Microsoft Windows. [CVADHELP-16017]
- Al presionar las teclas **Alt** + **Tab** en una sesión de usuario, es posible que se abra una nueva ventana vacía de la aplicación Citrix Workspace para Windows. [CVADHELP-16379]
- Es posible que la tecla **Imprimir pantalla** no haga capturas de pantalla, aunque se hayan minimizado las ventanas protegidas. [RFWIN-16777]
- Si está utilizando una cámara web o un vídeo en una llamada de Microsoft Teams, es posible que `HDXrtcengine.exe` deje de responder. Como solución temporal, consulte el artículo CTX296639 de Knowledge Center. [HDX-29122]
- Al intentar componer texto DBCS con un editor IME, es posible que falten subrayados. El problema se produce con los sistemas operativos Windows 10 2004. [RFWIN-20006]
- Es posible que los permisos establecidos incorrectamente en la carpeta `C:\ProgramData\Citrix` provoquen que la aplicación Citrix Workspace se cierre de manera inesperada. [RFWIN-22753]
- Durante las videollamadas de Microsoft Teams, es posible que el LED de la cámara parpadee y que el vídeo de vista previa se detenga. [CVADHELP-16383]

### Interfaz de usuario

- Es posible que la aplicación Citrix Workspace para Windows no se cierre al hacer clic una vez en la opción Salir. Como solución temporal, seleccione la opción Salir dos veces para que la aplicación Workspace se cierre. [RFWIN-21518]

Para ver los problemas existentes en el producto, consulte la sección Problemas conocidos.

## 2102

### Novedades

#### Compatibilidad con la autenticación de proxy

Antes, en máquinas cliente configuradas con autenticación de proxy, si las credenciales del proxy no existían en el **Administrador de credenciales de Windows**, no se le permitía autenticarse en la aplicación Citrix Workspace.

Ahora, en las máquinas cliente configuradas para la autenticación de proxy, si las credenciales de proxy no se almacenan en el **Administrador de credenciales de Windows**, aparece un mensaje de autenticación en el que se le pide que introduzca las credenciales del proxy. A continuación, la aplicación Citrix Workspace guarda las credenciales del servidor proxy en el **Administrador de credenciales de Windows**. Esto simplifica la experiencia de inicio de sesión porque no necesita guardar manualmente las credenciales en el Administrador de credenciales de Windows antes de acceder a la aplicación Citrix Workspace.

### Mejoras de Microsoft Teams

- Generación de vídeo mejorada.
- Mejoras en el rendimiento y la fiabilidad.

### Problemas resueltos

#### Sesión/Conexión

- Al intentar abrir una aplicación desde **Favoritos** en un escritorio publicado mediante la aplicación Citrix Workspace con la opción vPrefer habilitada, es posible que la aplicación se abra con un círculo giratorio. Si el círculo giratorio no desaparece, no puede volver a abrir la aplicación. [CVADHELP-13237]
- Con la opción vPrefer habilitada, es posible que las aplicaciones de App-V se inicien en un servidor remoto en lugar de iniciarse en un servidor local. [CVADHELP-15356]
- Es posible que el comando `StoreBrowse.exe` no muestre la lista completa de aplicaciones publicadas cuando los nombres de aplicación se indican en chino tradicional o en japonés. [CVADHELP-15952]
- Cuando el parámetro del Registro `EnableFactoryReset` está establecido en `False`, es posible que no se pueda desinstalar la aplicación Citrix Workspace y que aparezca este mensaje de error:

  Esta función ha sido inhabilitada.

  [CVADHELP-16114]

- Es posible que la función de recopilación de registros no recopile el rastro CDF. [CVADHELP-16587]

#### Excepciones del sistema

- El proceso `Receiver.exe` puede cerrarse inesperadamente. [CVADHELP-15669]

#### Interfaz de usuario

- Al usar el Editor de métodos de entrada (IME) chino o japonés para escribir en un cuadro de texto, es posible que el texto aparezca fuera del cuadro de texto en la esquina superior izquierda de la pantalla. [CVADHELP-15614]

Para ver los problemas existentes en el producto, consulte la sección Problemas conocidos.

### 2012.1

#### Novedades

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

#### Problemas resueltos

- La actualización automática de la aplicación Citrix Workspace de la versión 2012 a una posterior falla y muestra este mensaje de error:

  “No se pudo cargar el archivo o ensamblar Newtonsoft.Json”

  El problema se produce solamente cuando se habilita la actualización automática en una instancia instalada por un administrador de la aplicación Citrix Workspace.

  Como solución temporal, descargue la versión 2012.1 de la aplicación Citrix Workspace o una posterior de la página Descargas de Citrix e instálela manualmente.

  [RFWIN-21715]

Para ver los problemas existentes en el producto, consulte la sección Problemas conocidos.

### 2012

#### Novedades

#### Idioma italiano disponible

Ahora, la aplicación Citrix Workspace para Windows está disponible en italiano.

### Recopilación de registros

La recopilación de registros simplifica el proceso de recopilación de registros para la aplicación Citrix Workspace. Los registros ayudan a Citrix a solucionar problemas y, en el caso de problemas complicados, facilitan la asistencia técnica.

Ahora puede recopilar registros mediante la GUI.

Para obtener más información, consulte Recopilación de registros.

### Autenticación PassThrough de dominio en Citrix Workspace

En esta versión, se introduce la autenticación PassThrough de dominio en Citrix Workspace, junto con la compatibilidad existente para StoreFront.

### Autenticación silenciosa para Citrix Workspace

La aplicación Citrix Workspace presenta una directiva de objeto de directiva de grupo (GPO) para habilitar la autenticación silenciosa en Citrix Workspace. Esta directiva permite a la aplicación Citrix Workspace iniciar sesión en Citrix Workspace automáticamente al iniciar el sistema. Utilice esta directiva solo cuando la autenticación PassThrough de dominio (Single Sign-On) esté configurada para Citrix Workspace en dispositivos unidos a un dominio.

Para obtener más información, consulte Autenticación silenciosa.

### Mejora de la configuración de protección de aplicaciones

Antes, el administrador de autenticación y los cuadros de diálogo de **Self-Service Plug-in** estaban protegidos de forma predeterminada.

En esta versión, se presenta una directiva de objeto de directiva de grupo (GPO) que permite configurar las funciones de protección contra el registro de tecleo y protección contra capturas de pantalla por separado para las interfaces del administrador de autenticación y del Self-Service Plug-in.

> **Nota:**
>
> Esta directiva de GPO no se aplica a las sesiones ICA y SaaS. Las sesiones ICA y SaaS se siguen controlando mediante el Delivery Controller y Citrix Secure Private Access.

Para obtener más información, consulte Mejora de la configuración de protección de aplicaciones.

### Mejoras de Microsoft Teams

- Ahora, los usuarios pueden ver el puntero del presentador en una sesión de pantalla compartida.

- El motor de medios WebRTC ahora tiene en cuenta el servidor proxy configurado en el dispositivo cliente.

### Problemas resueltos

#### Instalación, desinstalación y actualización

- Al intentar actualizar la aplicación Citrix Workspace mediante el acceso directo creado manualmente, es posible que este se elimine y vuelva a crearse. [CVADHELP-15397]

#### Sesión/Conexión

- En un entorno de varios monitores, puede que una sesión de usuario no se maximice. El problema se produce al volver a acoplar el portátil. [CVADHELP-13614]
- Es posible que aparezca un cuadro de diálogo de advertencia de seguridad al realizar una de las siguientes acciones:
  - Obtener un archivo ICA de StoreFront mediante el comando **Storebrowse**.
  - Iniciar una aplicación mediante un archivo ICA en lugar de hacerlo desde un explorador web.

  [CVADHELP-15221]
- En un caso de doble salto, es posible que no se pueda iniciar una aplicación mediante el acceso directo del menú Inicio. El problema se produce si se habilita el límite de una instancia de aplicación por usuario. [CVADHELP-15576]
- Configure la aplicación Citrix Workspace para Windows para conectarse a todas las cuentas de almacén al establecer una sesión. Si cierra sesión en la aplicación Citrix Workspace y vuelve a iniciar sesión, la configuración de la cuenta de almacén cambia a una cuenta de almacén en lugar de establecerse de forma predeterminada en todas las cuentas. [CVADHELP-15728]
- Es posible que, al intentar compartir la pantalla en llamadas de Microsoft Teams, se vea una pantalla negra. [HDX-27041]
- En las llamadas de Microsoft Teams, es posible que el audio suene entrecortado. El problema se produce cuando el puerto del tráfico UDP está inhabilitado. [HDX-27914]

#### Experiencia de usuario

- Puede que falle el inicio de sesión después de instalar o actualizar la aplicación Citrix Workspace para Windows. El inicio de sesión se atasca en la pantalla Preparando el escritorio. El problema se produce al configurar Desktop Lock desde una URL de Citrix Gateway.

> **Nota:**
>
> Aparece una pantalla en negro durante algún tiempo antes de que aparezca Desktop Lock la primera vez que se configura la aplicación Citrix Workspace para Windows desde una URL de Citrix Gateway y Desktop Lock. Si la pantalla negra sigue mostrándose durante mucho tiempo, cierre la sesión con Ctrl+Alt+Supr para máquinas físicas y Ctrl+Alt+Fin para máquinas virtuales.

[CVADHELP-15334]

- Con la opción PPP elevado establecida en Sí o No, al iniciar una sesión de escritorio, es posible que algunos elementos de la barra de herramientas del **visor del CD** no se escalen para que coincidan con la configuración actual de PPP del dispositivo. El problema se produce cuando la configuración de PPP del dispositivo del usuario es superior a 100%. [CVADHELP-15418]
- Después de actualizar la aplicación Citrix Workspace a la versión 1912 CU1 desde la versión 1912, la enumeración de aplicaciones puede ser lenta y tardar unos 10 minutos en completarse. [CVADHELP-15766]

Para ver los problemas existentes en el producto, consulte la sección Problemas conocidos.

## Problemas conocidos

### Problemas conocidos en la versión 2302

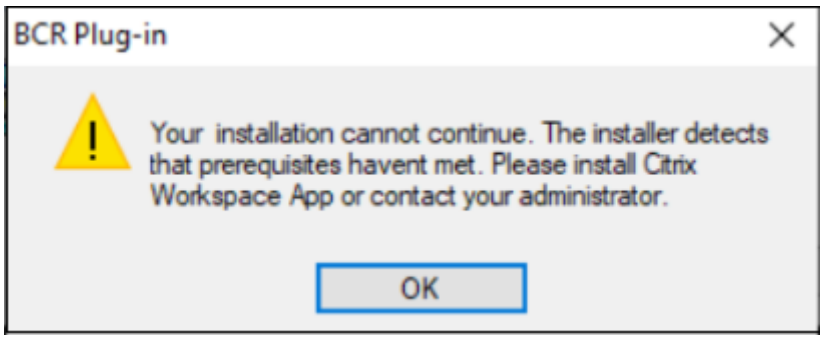
- Es posible que no pueda utilizar la aplicación Bloomberg Terminal con el teclado Bloomberg 5 o el teclado Bloomberg 2013. Este problema se produce cuando la versión 2302 de la aplicación Citrix Workspace está instalada en el sistema con la función de protección de aplicaciones habilitada. Como solución temporal, actualice la aplicación Citrix Workspace a la versión 2303 o cree esta clave de Registro y reinicie la máquina:
  - Clave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\epusbfilter
  - Valor: [DWORD]
  - DisableUSBFiltering= 1

  [CVADHELP-22221]

### Problemas conocidos en la versión 2212

- Cuando no se puede reparar el archivo BCRClient.msi, aparece el siguiente error durante la instalación de la aplicación Citrix Workspace:




[HDX-46964]

- Algunas aplicaciones SaaS que tienen la seguridad mejorada desactivada no se abren en Citrix Enterprise Browser cuando este es el explorador predeterminado. [CTXBR-4106]

#### Problemas conocidos en la versión 2210.5

- Al abrir una aplicación publicada en modo integrado, es posible que otras aplicaciones locales o integradas aparezcan en primer plano y tapen la aplicación publicada. [CVADHELP-20742]
- En algunas series antiguas de la GPU AMD, es posible que aparezca contenido de vídeo morado o pantallas parpadeantes con la aplicación Citrix Workspace 2206 o una versión posterior. Como solución temporal, modifique el registro siguiente:
  - Key: HKLM\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Gf
  - Value: [DWORD]
  - ForceVP= 1

  [HDX-46264]

#### Problemas conocidos en la versión 2210

- La barra de herramientas de **Desktop Viewer** podría cubrir la pantalla cuando el escritorio tiene una resolución y PPP normales. [HDX-45206]
- Es posible que la barra de herramientas de **Desktop Viewer** no aparezca correctamente en el modo de pantalla completa y que muestre las opciones en un orden incorrecto. [HDX-45189]
- Es posible que la posición y el tamaño de la ventana no se conserven al reconectar el escritorio. [HDX-44997]

#### Problemas conocidos en la versión 2209

No se han observado nuevos problemas en esta versión.

#### Problemas conocidos en 2207

No se han observado nuevos problemas en esta versión.

#### Problemas conocidos en la versión 2206

No se han observado nuevos problemas en esta versión.

#### Problemas conocidos en la versión 2205

- En la aplicación Citrix Workspace para Windows, la codificación de audio avanzada (AAC) solo admite un máximo de 6 canales. [CTXBR-2941]
- Al conectar un dispositivo USB o acceder a archivos, es posible que la aplicación Citrix Workspace muestre el cuadro de diálogo antiguo **Citrix Workspace: Advertencia de seguridad**. [LCM-10369]
- Es posible que la notificación del estado de la batería y el cuadro de diálogo emergente del teclado automático no aparezcan durante la sesión cuando la directiva **Visualización automática del teclado** está habilitada en el DDC. [HDX-39558]

#### Problemas conocidos en la versión 2204.1

- La instalación de la aplicación Citrix Workspace para Windows en modo sin conexión puede fallar cuando el instalador no encuentra Microsoft Edge WebView2 en el sistema.

  Como solución temporal, instale **MicrosoftEdgeWebView2RuntimeInstallerX86.exe** como administrador y, a continuación, instale la aplicación Citrix Workspace para Windows.

  [RFWIN-26329]

#### Problemas conocidos en la versión 2202

- Es posible que una nueva instalación o actualización de la aplicación Citrix Workspace provoque una demora de entre 10 y 30 minutos. Para obtener más información, consulte el artículo CTX335639 de Citrix Knowledge Center. [RFWIN-25752]

#### Problemas conocidos en la versión 2112.1

- Es posible que la tecla Imprimir pantalla no realice capturas de pantalla cuando la aplicación Citrix Workspace para Windows con la protección de aplicaciones habilitada se inicia en segundo plano. [RFWIN-25835]

- Es posible que una nueva instalación o actualización de la aplicación Citrix Workspace provoque una demora de entre 10 y 30 minutos. Para obtener más información, consulte el artículo CTX335639 de Citrix Knowledge Center. [RFWIN-25752]
- Es posible que no se cierre sesión correctamente de la aplicación Citrix Workspace para Windows cuando la autenticación proxy está habilitada. [RFWIN-24813]
- Si utiliza la aplicación Citrix Workspace en máquinas con Microsoft Windows 11, es posible que falten las fichas **Feed de actividades** y **Acciones**. [WSP-13311]
- Al utilizar Citrix Enterprise Browser, no se pueden tomar capturas de pantalla de ventanas con URL desprotegidas, ni siquiera cuando se minimizan las ventanas protegidas. [CTXBR-1925]
- Si habilitó la redirección de contenido del explorador web, no podrá iniciar sesión en Google Meet. [HDX-34649]
  Como solución alternativa:
  1. Asegúrese de que https://www.youtube.com/* esté disponible en la lista de control de acceso.
  2. Asegúrese de que https://accounts.google.com/* esté en la lista de sitios de autenticación.
  3. Inicie sesión en su cuenta de Google en cualquier sitio intermediario de Google, como, por ejemplo, YouTube.
  4. Desde la misma instancia de Google Chrome, inicie Google Meet.
- En la aplicación Citrix Workspace 2112.1, es posible que vea un uso elevado de la CPU en el dispositivo de punto final cuando la cámara web está encendida en videollamadas de Microsoft Teams optimizado.
  Como solución temporal, cree este valor del Registro en su dispositivo de punto final:

  Computer\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream
  Nombre: UseDefaultCameraConfig
  Tipo: REG_DWORD
  Valor: 0

  [HDX-37168]
- En la aplicación Citrix Workspace, es posible que se produzcan errores intermitentes al responder o realizar llamadas de Microsoft Teams. Aparece el siguiente mensaje de error:

  **No se pudo establecer la llamada.**

  Como solución temporal, intente establecer de nuevo la llamada de Microsoft Teams.

  [HDX-38819]

### Problemas conocidos en la versión 2109.1

No se han observado nuevos problemas en esta versión.

#### Problemas conocidos en la versión 2109

Si instaló la aplicación Workspace con una versión anterior a 2109 como usuario y el administrador instala la versión 21.0.9, aparece el mensaje de error **Entry point not found** si vuelve a iniciar sesión en el dispositivo como usuario. Si hace clic en **Aceptar**, el mensaje desaparece y la aplicación Workspace se actualiza a la versión 21.0.9. [RFWIN-25008]

Si el administrador instaló extensiones externas en Google Chrome, Citrix Enterprise Browser se cierra de forma inesperada al abrirlo. [CTXBR-2135]

#### Problemas conocidos en la versión 2108

Las sesiones no se pueden iniciar en el modo sin conexión (Continuidad del servicio) en las máquinas cliente cuando el nombre de usuario tiene caracteres en cirílico o en un idioma del este asiático. [RFWIN-23906]

#### Problemas conocidos en la versión 2107

No se han observado nuevos problemas en esta versión.

#### Problemas conocidos en la versión 2106

- En los almacenes en los que está habilitada la función Continuidad del servicio, es posible que no puedan iniciar recursos. El problema se produce con usuarios en Unicode. [RFWIN-23439]
- Al intentar redirigir una cámara web mediante la aplicación Citrix Workspace para Windows instalada en un VDA, es posible que la cámara falle. [HDX-28691]

#### Problemas conocidos en la versión 2105

- Durante una sesión, al hacer clic en **Buscar actualizaciones** y las actualizaciones se descargan correctamente, las sesiones actuales no aparecen en el cuadro de diálogo **Descarga correcta**. [RFWIN-23152]

#### Problemas conocidos en la versión 2103.1

- La ventana de Self-Service Plug-in está vacía y no se muestran aplicaciones al iniciar la sesión. El problema se produce al utilizar la tarjeta gráfica Intel Xe y por limitación de terceros. [CVADHELP-17005]
- Es posible que no se puedan componer caracteres correctamente en el editor IME japonés, chino o coreano. La ventana de redacción aparece desplazada y no está integrada. Este problema no se produce cuando se usan sesiones de aplicaciones y escritorios virtuales ni aplicaciones SaaS. [RFWIN-21158]

- Es posible que no se pueda salir de la aplicación Citrix Workspace. El problema se produce cuando la solicitud de credenciales de usuario aparece repetidamente. [RFWIN-22491]
- Después de crear un acceso directo de escritorio para una aplicación y reiniciar el dispositivo cliente, es posible que no se pueda iniciar la aplicación desde el acceso directo la primera vez. El problema se produce cuando no se especifica `storedescription` al instalar la aplicación Citrix Workspace mediante la interfaz de línea de comandos. [RFWIN-22510]
- Al descargar un archivo TXT de Citrix Files, es posible que el nombre del archivo en japonés no se pueda leer. [RFWIN-22516]
- Al intentar realizar una llamada entre dos usuarios con la optimización de HDX para Microsoft Teams, es posible que las llamadas fallen. Este problema se produce si la versión del VDA es 2103 o una anterior y la aplicación Workspace para Windows es 2103 o una posterior. Este problema está resuelto en Virtual Delivery Agent (VDA) 2106.

#### Problemas conocidos en la versión 2102

- Es posible que no se puedan iniciar sesiones ICA. El problema se produce cuando el servidor proxy utiliza el puerto 8080 en lugar de un puerto personalizado. [CVADHELP-15977]
- En una sesión de aplicación, al abrir una imagen para escanear en Microsoft Paint, es posible que tanto la aplicación Microsoft Paint como el proceso de escaneo dejen de responder. El problema se produce al iniciar la sesión en el modo de ventana. [RFWIN-21413]
- En las máquinas configuradas para la autenticación de varios factores (MFA) de Azure Active Directory, la solicitud de inicio de sesión aparece incluso tras seleccionar las opciones **Mantener mi sesión iniciada** y **No volver a preguntar durante 60 días**. [RFWIN-21623]
- Es posible que no se pueda iniciar sesión en la aplicación Citrix Workspace en máquinas unidas a Azure Active Directory. El problema se produce cuando no aparece la solicitud de autenticación. [RFWIN-21624]
- Al iniciar una sesión de escritorio publicada, aparece el cuadro de diálogo de Self-Service Plug-in en primer plano. El problema se produce cuando la directiva **Acceso a aplicaciones locales** está habilitada en el Delivery Controller. [RFWIN-21629]
- Es posible que, al intentar cambiar de ventana con las teclas **ALT** + **Tab**, la pantalla de la aplicación Citrix Workspace se quede vacía. El problema se produce al iniciar la sesión en el modo de ventana. [RFWIN-21828]
- Si utiliza una cámara web o vídeo en una llamada de Microsoft Teams, es posible que `HDXrtcengine.exe` deje de responder. Como solución temporal, consulte el artículo CTX296639 de Knowledge Center. [HDX-29122]

#### Problemas conocidos en la versión 2012.1

No se han observado nuevos problemas en esta versión.

#### Problemas conocidos en la versión 2012

- Si intenta agregar una aplicación protegida a **Favoritos**, es posible que aparezca este mensaje: "Sus aplicaciones no están disponibles en este momento". Al hacer clic en **Aceptar**, aparece este otro mensaje: "No se puede agregar la aplicación". Después de cambiar a la pantalla **Favoritos**, la aplicación protegida aparece allí, pero no puede quitarla de **Favoritos**. [WSP-5497]
- En el explorador Chrome con redirección de contenido del explorador, al hacer clic en un enlace que abre una nueva ficha, es posible que esta no se abra. Como solución temporal, seleccione la opción para **permitir siempre las ventanas emergentes y redirecciones** en el mensaje de **bloqueo de ventanas emergentes**. [HDX-23950]
- La actualización automática de la aplicación Citrix Workspace de la versión 2012 a una posterior falla y muestra este mensaje de error:

  **No se pudo cargar el archivo o ensamblar Newtonsoft.Json**

  El problema se produce solamente cuando se habilita la actualización automática en una instancia instalada por un administrador de la aplicación Citrix Workspace.

  Como solución temporal, descargue la versión 2012.1 de la aplicación Citrix Workspace o una posterior de la página Descargas de Citrix e instálela manualmente.

  [RFWIN-21715]
- Si inicia la barra de aplicaciones y, a continuación, abre el menú **Central de conexiones** en la aplicación Citrix Workspace para Windows, la barra de aplicaciones no aparece en el servidor que la aloja. [HDX-27504]
- Si utiliza la aplicación Citrix Workspace para Windows e inicia la barra de aplicaciones en posición vertical, la barra cubre el menú Inicio o el reloj de la bandeja del sistema. [HDX-27505]

### Documentación antigua

Para ver las versiones de productos que han alcanzado el fin de su vida (EOL), consulte Documentación antigua.

### Avisos de terceros

Es posible que la aplicación Citrix Workspace incluya software de terceros con licencias definidas en los términos del siguiente documento:

Avisos legales de terceros de la aplicación Citrix Workspace para Windows (descarga de PDF)

# Requisitos del sistema y compatibilidad

February 21, 2023

## Requisitos

- Mínimo 1 GB de RAM.
- En la tabla siguiente se indica el espacio necesario en el disco para instalar la aplicación Citrix Workspace.

| Tipo de instalación | Espacio de disco requerido |
|---|---|
| Instalación nueva | 572 MB |
| Actualización de versión | 350 MB |

> **Nota:**
>
> - El instalador solo lleva a cabo la comprobación de espacio en el disco después de haberse extraído el paquete de instalación.
> - Cuando el sistema tiene poco espacio en el disco durante una instalación silenciosa, no aparece el cuadro de diálogo, pero se registra el mensaje de error en `CTXInstall \\_TrolleyExpress-\*.log`.

- Versión 102 de Microsoft Edge WebView2 Runtime o una posterior.

> **Nota:**
>
> A partir de la versión 2107 de la aplicación Citrix Workspace, Microsoft Edge WebView2 Evergreen Bootstrapper se incluye con el instalador de la aplicación Citrix Workspace. Evergreen Bootstrapper es el pequeño instalador que descarga la versión de WebView2 Runtime que coincide con la arquitectura del dispositivo y la instala localmente.
>
> Durante la instalación de la aplicación Workspace, el instalador comprueba si Microsoft Edge WebView2 Runtime está presente en el sistema y, si no lo encuentra, lo instala.
>
> **Debe tener conexión a Internet para descargar e instalar Microsoft Edge WebView2 Runtime.**
>
> Al intentar instalar o actualizar la versión de la aplicación Citrix Workspace con privilegios que no son de administrador y Microsoft Edge WebView2 Runtime no está presente, la instalación se detiene con este mensaje:

> "Debe iniciar sesión como administrador para instalar estos paquetes de requisitos previos:
>
> Edge Webview2 Runtime"

- Self-Service Plug-in requiere .NET 4.8. Permite suscribirse e iniciar aplicaciones y escritorios desde la línea de comandos o la interfaz de usuario de la aplicación Workspace.

  Al intentar instalar o actualizar la versión de la aplicación Citrix Workspace a la versión 1904 o a una posterior y la versión requerida de .NET Framework no está disponible en su sistema Windows, el instalador de la aplicación Citrix Workspace descarga e instala la versión requerida de .NET Framework.

  > **Nota:**
  >
  > Se produce un error en la instalación al intentar instalar o actualizar la versión de la aplicación Citrix Workspace con privilegios que no son de administrador y .NET Framework 4.8 o una versión más reciente no está presente en el sistema.

- La versión más reciente de Microsoft Visual C++ Redistributable.

  > **Nota:**
  >
  > Citrix recomienda utilizar la versión más reciente de Microsoft Visual C++ Redistributable. De lo contrario, es posible que aparezca un mensaje de reinicio durante la actualización de versiones.

  A partir de la versión 1904, el instalador de Microsoft Visual C++ Redistributable se empaqueta con el instalador de la aplicación Citrix Workspace. Durante la instalación de la aplicación Workspace, el instalador comprueba si el paquete de Microsoft Visual C++ Redistributable está presente en el sistema y lo instala si es necesario.

  > **Nota:**
  >
  > Si el paquete de Microsoft Visual C++ Redistributable no existe en el sistema, es posible que falle la instalación de la aplicación Citrix Workspace con privilegios que no son de administrador.

  Solamente un administrador puede instalar el paquete Microsoft Visual C++ Redistributable.

  Para solucionar problemas con la instalación de .NET Framework o Microsoft Visual C++ Redistributable, consulte el artículo CTX250044 de Citrix Knowledge Center.

> **Nota:**
>
> **Debe tener conexión a Internet para descargar e instalar .NET Framework y Microsoft Visual C++ Redistributable. De lo contrario, el administrador puede instalar estos requisitos mediante un método de implementación, como, por ejemplo, SCCM.**

### Tabla de compatibilidad

La aplicación Citrix Workspace es compatible con todas las versiones actualmente compatibles de Citrix Virtual Apps and Desktops, Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) y Citrix Gateway, según se indica en la tabla Citrix Product Lifecycle Matrix.

> **Nota:**
>
> - El plug-in del análisis de punto final (EPA) de Citrix Gateway está disponible en Citrix Workspace. En la aplicación nativa de Citrix Workspace, solo se ofrece al utilizar la autenticación nFactor. Para obtener más información, consulte Configure pre-auth and post-auth EPA scan as a factor in nFactor authentication en la documentación de Citrix ADC.
> - La instalación de la aplicación Citrix Workspace en Windows solo se admite cuando los clientes cuentan con asistencia y mantenimiento generales o ampliados de Microsoft.
> - La aplicación Citrix Workspace para Windows solamente se admite en modo de emulación en el sistema operativo Windows ARM64.
> - Una vez que una versión de Windows 10 haya alcanzado la finalización del servicio, Microsoft ya no ofrece desarrollo adicional ni servicios para dicha versión. Citrix ofrece asistencia para su software solamente en sistemas operativos que su fabricante siga manteniendo. Para obtener información sobre la finalización del servicio de Windows 10, consulte las Preguntas frecuentes sobre el ciclo de vida: Windows de Microsoft.

La aplicación Citrix Workspace para Windows es compatible con los siguientes sistemas operativos Windows:

| Sistema operativo |
| --- |
| Windows 11 |
| Windows 10 Enterprise (ediciones de 32 y 64 bits). Para obtener más información sobre las versiones compatibles de Windows 10, consulte Compatibilidad de Windows 10 con la aplicación Citrix Workspace para Windows. |
| Windows 10 Enterprise (2016 LTSB 1607, LTSC 2019) |
| Windows 10 (Home Edition*, Pro) |
| Windows Server 2022 |
| Windows Server 2019 |
| Windows Server 2016 |

*No se admite la autenticación PassThrough de dominio, Desktop Lock, la API de FastConnect ni configuraciones que requieran una máquina Windows unida a un dominio.

**Compatibilidad de Windows 10 u 11 con la aplicación Citrix Workspace para Windows**

En esta tabla, se muestra el número de la versión de Windows 10 y las correspondientes versiones compatibles de la aplicación Citrix Workspace para Windows.

| Número de versión de Windows 10 | Número de compilación | Versión de la aplicación Citrix Workspace |
|---|---|---|
| 22H2 | 19045 | 2206 y versiones posteriores |
| 21H2 | 19044 | 2112.1 y versiones posteriores |
| 21H1 | 19043.928 | 2106 y versiones posteriores |
| 20H2 | 19042.508 | 2012 y versiones posteriores |
| 2004 | 19041.113 | 2006.1 y versiones posteriores |
| 1909 | 18363.418 | 1911 y versiones posteriores |
| 1903 | 18362.116 | 1909 y versiones posteriores |
| 1809 | 17763.107 | 1812 y versiones posteriores |
| 1803 | 17134.376 | 1808 y versiones posteriores |

> **Nota:**
>
> Las versiones de Windows 10 son compatibles solamente con las versiones mencionadas de la aplicación Citrix Workspace. Por ejemplo, la versión 21H1 de Windows 10 no es compatible con la versión anterior a 2106.

En esta tabla, se muestra el número de la versión de Windows 11 y las correspondientes versiones compatibles de la aplicación Citrix Workspace para Windows.

| Número de versión de Windows 11 | Número de compilación | Versión de la aplicación Citrix Workspace |
|---|---|---|
| 22H2 | 22621 | 2209 y versiones posteriores |
| 21H2 | 22000 | 2109.1 y versiones posteriores |

## Instalación y desinstalación

March 31, 2023

Dispone de las siguientes maneras de instalar la aplicación Citrix Workspace:

- Puede descargar el paquete de instalación `CitrixWorkspaceApp.exe` desde la página Descargas.
- O bien desde la página de descargas de la empresa (si está disponible).

Puede instalar el paquete de la siguiente manera:

- Ejecute un asistente de instalación interactivo basado en Windows. O bien:
- Escriba el nombre de archivo del instalador, los comandos de instalación y las propiedades de instalación en la interfaz de la línea de comandos. Para obtener información sobre cómo instalar la aplicación Citrix Workspace mediante la interfaz de la línea de comandos, consulte Usar parámetros de la línea de comandos.

**Instalar con y sin privilegios de administrador:**

Tanto los usuarios como los administradores pueden instalar la aplicación Citrix Workspace. Los privilegios de administrador solo se requieren cuando se usa la autenticación PassThrough y Citrix Ready Workspace Hub con la aplicación Citrix Workspace para Windows.

En la siguiente tabla se describen las diferencias cuando un administrador o usuario instalan la aplicación Citrix Workspace:

| | Carpeta de instalación | Tipo de instalación |
|---|---|---|
| Administrador | C:\Archivos de programa (x86)\Citrix\ICA Client | Instalación por sistema |
| Usuario | %USERPROFILE%\AppData\Local\Citrix\ICA Client | Instalación por usuario |

> **Nota:**
>
> Los administradores pueden supeditar la instancia instalada por el usuario de la aplicación Citrix Workspace y continuar con la instalación correctamente.

### Usar un instalador basado en Windows

Para instalar la aplicación Citrix Workspace para Windows, ejecute manualmente el paquete del instalador de `CitrixWorkspaceApp.exe` siguiendo estos métodos:

- Medios de instalación
- Recurso compartido de red
- Explorador de Windows
- Interfaz de la línea de comandos

De forma predeterminada, los registros del instalador se encuentran en esta ubicación:

- En el sistema operativo Windows de 32 bits: `C:\Program Files\Citrix\Logs`
- En el sistema operativo Windows de 64 bits: `C:\Program Files (x86)\Citrix\Logs` o `C:\Users\<Install Username>\AppData\Local\Temp`

1. Inicie el archivo `CitrixWorkspaceApp.exe` y haga clic en **Inicio**.
2. Lea y acepte el Contrato de licencia de usuario final y continúe con la instalación.
3. Cuando se instala en una máquina unida a un dominio con privilegios de administrador, aparece un cuadro de diálogo de inicio de sesión Single Sign-On. Consulte Autenticación PassThrough de dominio para obtener más información.
4. Siga las instrucciones del instalador basado en Windows para completar la instalación.

Cuando se completa la instalación, la aplicación Citrix Workspace solicita que agregue una cuenta. Para obtener información sobre cómo agregar cuentas, consulte Agregar cuentas o cambiar de servidor.

### Usar parámetros de línea de comandos

Puede personalizar el instalador de la aplicación Citrix Workspace. Para ello, especifique las opciones pertinentes en la línea de comandos. El paquete de instalación se descomprime automáticamente en el directorio temporal del sistema antes de iniciar el programa de instalación. El requisito de espacio incluye espacio para archivos de programa, datos de usuarios y directorios temporales después de iniciar varias aplicaciones.

Para instalar la aplicación Citrix Workspace desde la línea de comandos de Windows, inicie el símbolo del sistema y escriba lo siguiente en la misma línea:

- Nombre del archivo del instalador
- Comandos de instalación
- Y propiedades de instalación

Los comandos y las propiedades de instalación disponibles son los siguientes:

```
CitrixWorkspaceApp.exe [commands] [properties]
```

### Lista de parámetros de la línea de comandos

Los parámetros se pueden clasificar, a grandes rasgos, de la siguiente manera:

- Parámetros comunes
- Parámetros de instalación
- Parámetros de funciones HDX
- Parámetros de preferencias e interfaz de usuario
- Parámetros de autenticación

#### Parámetros comunes

- /? o /help: Enumera todos los comandos y propiedades de instalación.
- /silent: Inhabilita los cuadros de diálogo y solicitudes de instalación durante la instalación.
- /noreboot: Suprime las solicitudes de reinicio durante la instalación. Cuando elimina las solicitudes de reinicio, no se reconocen aquellos dispositivos USB que estén en estado suspendido. Los dispositivos USB se activan solo después de reiniciar el dispositivo.
- /includeSSON: Requiere que lleve a cabo la instalación como administrador. Indica que la aplicación Citrix Workspace se instalará con el componente Single Sign-On. Consulte Autenticación PassThrough de dominio para obtener más información.
- /forceinstall: Este modificador es efectivo al limpiar cualquier configuración existente o entradas de la aplicación Citrix Workspace que hubiera en el sistema. Utilice este modificador en los siguientes casos:
  - Al actualizar una versión de la aplicación Citrix Workspace no compatible.
  - La instalación o la actualización no se han realizado correctamente.

  > **Nota:**
  >
  > El modificador /forceinstall reemplaza al modificador /rcu. El modificador /rcu se retiró en la versión 1909. Para obtener más información, consulte Elementos retirados.

#### Parámetros de instalación

##### /AutoUpdateCheck

Indica que la aplicación Citrix Workspace detecta si hay una actualización disponible.

> **Nota:**
>
> /AutoUpdateCheck es un parámetro obligatorio que debe definir para configurar otros parámetros como /AutoUpdateStream, /DeferUpdateCount o /AURolloutPriority.

- Automático (predeterminado): Se le notificará cuando haya una actualización disponible. Por ejemplo: CitrixWorkspaceApp.exe /AutoUpdateCheck=auto.
- Manual: No se le notificará cuando haya actualizaciones disponibles. Compruebe manualmente si hay actualizaciones. Por ejemplo: CitrixWorkspaceApp.exe /AutoUpdateCheck=manual.
- Disabled: Inhabilita las actualizaciones automáticas. Por ejemplo: CitrixWorkspaceApp.exe /AutoUpdateCheck=disabled.

### /AutoUpdateStream

Si habilitó la actualización automática, puede elegir la versión que quiere actualizar. Consulte Hitos del ciclo de vida para obtener más información.

- LTSR: Actualizaciones automáticas solamente para actualizaciones Long Term Service Release Cumulative Updates. Por ejemplo: `CitrixWorkspaceApp.exe /AutoUpdateStream=LTSR`.
- Current: Actualizaciones automáticas para la versión más reciente de la aplicación Citrix Workspace. Por ejemplo: `CitrixWorkspaceApp.exe /AutoUpdateStream=Current`.

### /DeferUpdateCount

Indica las veces que puede aplazar las notificaciones cuando haya una actualización disponible. Para obtener más información, consulte Actualizaciones de Citrix Workspace.

- -1 (valor predeterminado): Permite aplazar las notificaciones tantas veces como quiera. Por ejemplo: `CitrixWorkspaceApp.exe /DeferUpdateCount=-1`.
- 0: Indica que recibirá (solo) una notificación por cada actualización disponible. No le recuerda de nuevo la actualización. Por ejemplo: `CitrixWorkspaceApp.exe /DeferUpdateCount=0`.
- Cualquier otro número “n”: Permite aplazar las notificaciones “n” veces. La opción **Recordármelo más tarde** se podrá mostrar tantas veces como indique el valor “n”. Por ejemplo: `CitrixWorkspaceApp.exe /DeferUpdateCount=<n>`.

### /AURolloutPriority

Cuando hay disponible una nueva versión de la aplicación, Citrix implanta la actualización durante un período de entrega específico. Con este parámetro, puede controlar el momento del período de entrega en que puede recibir la actualización.

- Auto (valor predeterminado): Recibe las actualizaciones durante el período de entrega configurado por Citrix. Por ejemplo: `CitrixWorkspaceApp.exe /AURolloutPriority=Auto`.
- Fast: Recibe las actualizaciones al comienzo del período de entrega. Por ejemplo: `CitrixWorkspaceApp.exe /AURolloutPriority=Fast`.
- Medium: Recibe las actualizaciones a mitad del período de entrega. Por ejemplo: `CitrixWorkspaceApp.exe /AURolloutPriority=Medium`.
- Slow: Recibe las actualizaciones al final del período de entrega. Por ejemplo: `CitrixWorkspaceApp.exe /AURolloutPriority=Slow`.

### /startAppProtection

Inicia el componente Protección de aplicaciones y proporciona una seguridad mejorada porque restringe la posibilidad de que los clientes corran peligro por parte de malware que registra las pulsaciones de teclas y captura pantallas.

- `CitrixWorkspaceApp.exe /startAppProtection`

Consulte Protección de aplicaciones para obtener más información.

> **Nota:**
>
> El modificador `/startAppProtection` reemplaza al modificador `/includeAppProtection`. El modificador `/includeAppProtection` se retiró en la versión 2212. Para obtener más información, consulte Elementos retirados.

### /InstallEmbeddedBrowser

Excluye los binarios del explorador integrado de Citrix. Ejecute el modificador `/InstallEmbeddedBrowser=N` para excluir la función del explorador integrado.

Puede excluir los binarios del explorador integrado de Citrix solo en los siguientes casos:

- Instalación nueva
- Actualice una versión que no incluya los binarios del explorador integrado de Citrix.

Si la versión de la aplicación Citrix Workspace incluye los binarios del explorador integrado de Citrix y usted va a actualizar a la versión 2002, los binarios del explorador integrado se actualizan automáticamente durante la actualización.

### INSTALLDIR

Especifica el directorio de instalación personalizado para la instalación de la aplicación Citrix Workspace. La ruta predeterminada es `C:\Program Files\Citrix`. Por ejemplo: `CitrixWorkspaceApp.exe INSTALLDIR=C:\Program Files\Citrix`.

### /IncludeCitrixCasting

Instala Citrix Casting durante la instalación.

> **Nota:**
>
> Al actualizar la aplicación Citrix Workspace, Citrix Casting se actualiza automáticamente. Para obtener más información sobre Citrix Casting, consulte Citrix Casting.

### ADDLOCAL

Utilice la clave ADDLOCAL para instalar uno o varios componentes específicos de la aplicación Citrix Workspace. Con esta clave, si instala algún componente específico, la aplicación Citrix Workspace instala todos los componentes obligatorios de forma predeterminada.

> **Nota:**
>
> Le recomendamos que utilice la clave ADDLOCAL solo si quiere instalar alguno de los componentes específicos de la aplicación Citrix Workspace. De forma predeterminada, si no se especifica ningún parámetro ADDLOCAL, se instalan todos los componentes compatibles durante la instalación de la aplicación Citrix Workspace.

En la siguiente tabla se enumeran los componentes compatibles con la clave ADDLOCAL:

| Clave ADDLOCAL | Nombre del componente | Descripción |
|---|---|---|
| ReceiverInside | Receiver | Proporciona los servicios del SDK de Workspace a Self-service plug-in. |
| ICA_Client | Motor HDX | Este componente gestiona el proceso de inicio de sesión o archivo ICA. |
| BCR_Client | Cliente BCR | Plug-in para gestionar la redirección de contenido del explorador. |
| USB | Cliente USB | Plug-in para realizar la redirección USB. |
| DesktopViewer | Cliente Desktop Viewer | Marco de interfaz de usuario para escritorio virtual. |
| AM | AuthManager | Administrador de autenticación: Autoriza al usuario a acceder a la aplicación Citrix Workspace. |
| SSON | SSON | Componente Single Sign-On: Admite Single Sign-On (SSO). |
| SELFSERVICE | Self-service | Plug-in para inicio nativo de Citrix Workspace. |
| WebHelper | Web Helper | Ayudante para conectar el explorador con la aplicación de espacio de trabajo nativa. |

| Clave ADDLOCAL | Nombre del componente | Descripción |
|---|---|---|
| WorkspaceHub | Win Docker | Proporciona una forma de ampliar el espacio de trabajo del usuario, duplicando o ampliando la pantalla local de forma inalámbrica. |
| CitrixEnterpriseBrowser | Explorador web | Explorador nativo que permite a los usuarios abrir aplicaciones web o SaaS desde la aplicación Citrix Workspace de forma segura. |

Por ejemplo, con el siguiente comando, puede instalar los componentes mencionados en el comando:

```
CitrixWorkspaceapp.exe ADDLOCAL=ReceiverInside,ICA_Client,BCR_Client,
    USB,DesktopViewer,AM,SSON,SelfService,WebHelper,WorkspaceHub,
    CitrixEnterpriseBrowser
<!--NeedCopy-->
```

> **Nota:**
>
> A partir de la versión 2212, la función de protección de aplicaciones se instala de forma predeterminada. Como resultado, AppProtection ya no es una opción válida para ADDLOCAL.

### Parámetros de funciones HDX

#### ALLOW_BIDIRCONTENTREDIRECTION

Indica si la redirección de contenido bidireccional entre el cliente y el host está habilitada. Para obtener más información, consulte la sección Configuraciones de directiva de Redirección de contenido bidireccional en la documentación de Citrix Virtual Apps and Desktops.

- 0 (valor predeterminado): Indica que la redirección bidireccional de contenido está inhabilitada. Por ejemplo: CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=0.
- 1: Indica que la redirección bidireccional de contenido está habilitada. Por ejemplo: CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=1.

#### FORCE_LAA

Indica que la aplicación Citrix Workspace está instalada con el componente de acceso a aplicaciones locales del cliente. Instale la aplicación Workspace con privilegios de administrador para que este

componente funcione. Consulte la sección Acceso a aplicaciones locales en la documentación de Citrix Virtual Apps and Desktops para obtener más información.

- 0 (predeterminado): Indica que el componente de acceso a aplicaciones locales no está instalado. Por ejemplo: `CitrixWorkspaceApp.exe FORCE_LAA =0`.
- 1: Indica que el componente de acceso a aplicaciones locales del cliente está instalado. Por ejemplo: `CitrixWorkspaceApp.exe FORCE_LAA =1`.

#### LEGACYFTAICONS

Especifica si quiere mostrar iconos de documentos o archivos que tienen asociaciones de tipo de archivo con aplicaciones suscritas.

- False (valor predeterminado): Muestra iconos de documentos o archivos que tienen asociaciones de tipo de archivo con aplicaciones suscritas. Cuando se establece en "false", el sistema operativo genera un icono para el documento que no tiene asignado un icono específico. El icono generado por el sistema operativo es un icono genérico superpuesto con una versión más pequeña del icono de la aplicación. Por ejemplo: `CitrixWorkspaceApp.exe LEGACYFTAICONS=False`.
- True: No muestra iconos de documentos o archivos que tienen asociaciones de tipo de archivo con aplicaciones suscritas. Por ejemplo: `CitrixWorkspaceApp.exe LEGACYFTAICONS=True`.

#### ALLOW_CLIENTHOSTEDAPPSURL

Habilita la función de redirección de URL en el dispositivo del usuario. Consulte la sección Acceso a aplicaciones locales en la documentación de Citrix Virtual Apps and Desktops para obtener más información.

- 0 (predeterminado): inhabilita la función de redirección de URL en el dispositivo del usuario. Por ejemplo: `CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=0`.
- 1: Habilita la función de redirección de URL en el dispositivo del usuario. Por ejemplo: `CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=1`.

### Parámetros de preferencias e interfaz de usuario

#### ALLOWADDSTORE

Permite configurar los almacenes (HTTP o HTTPS) en función del parámetro especificado.

- S (predeterminado): Permite agregar o quitar solamente almacenes seguros (configurados con HTTPS). Por ejemplo: `CitrixWorkspaceApp.exe ALLOWADDSTORE=S`.

- A: Permite agregar o quitar tanto almacenes seguros (HTTPS) como no seguros (HTTP). No se aplica si la aplicación Citrix Workspace está instalada por usuario. Por ejemplo: `CitrixWorkspaceApp.exe ALLOWADDSTORE=A`.
- N: No permite nunca que los usuarios agreguen o quiten su propio almacén. Por ejemplo: `CitrixWorkspaceApp.exe ALLOWADDSTORE=N`.

#### ALLOWSAVEPWD

Permite guardar las credenciales del almacén de forma local. Este parámetro solo se aplica a los almacenes que utilizan el protocolo de la aplicación Citrix Workspace.

- S (predeterminado): Permite guardar contraseñas solamente para almacenes seguros (configurados con HTTPS). Por ejemplo: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=S`.
- N: No permite guardar contraseñas. Por ejemplo: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=N`.
- A: Permite que los usuarios guarden contraseñas tanto para almacenes seguros (HTTPS) como no seguros (HTTP). Por ejemplo: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=A`.

#### STARTMENUDIR

Especifica el directorio para los accesos directos en el menú Inicio.

- `<Directory Name>`: De forma predeterminada, las aplicaciones aparecen en **Inicio** > **Todos los programas**. Puede especificar la ruta relativa de los accesos directos en la carpeta `\Programs`. Por ejemplo, para colocar accesos directos en **Inicio** > **Todos los programas** > **Workspace**, especifique `STARTMENUDIR=\Workspace`.

#### DESKTOPDIR

Especifica el directorio para los accesos directos del escritorio.

> **Nota:**
>
> Cuando utilice la opción DESKTOPDIR, establezca la clave `PutShortcutsOnDesktop` en `True`.

- `<Directory Name>`: Puede especificar la ruta relativa de los accesos directos. Por ejemplo, para colocar accesos directos en **Inicio > Todos los programas > Workspace**, especifique `DESKTOPDIR=\Workspace`.

#### SELFSERVICEMODE

Controla el acceso a la interfaz de usuario de la aplicación Workspace en modo autoservicio.

- True: Indica que el usuario tiene acceso a la interfaz de usuario de autoservicio. Por ejemplo: `CitrixWorkspaceApp.exe SELFSERVICEMODE=True`.
- False: Indica que el usuario no tiene acceso a la interfaz de usuario de autoservicio. Por ejemplo: `CitrixWorkspaceApp.exe SELFSERVICEMODE=False`.

#### ENABLEPRELAUNCH

Controla el preinicio de sesiones. Consulte Tiempo de inicio de aplicaciones para obtener más información.

- True: Indica que el preinicio de sesiones está habilitado. Por ejemplo: `CitrixWorkspaceApp.exe ENABLEPRELAUNCH=True`.
- False: Indica que el preinicio de sesiones está inhabilitado. Por ejemplo: `CitrixWorkspaceApp.exe ENABLEPRELAUNCH=False`.

#### `DisableSetting`

Oculta la opción **Accesos directos y reconexión** para que no se muestre en la hoja **Preferencias avanzadas**. Consulte Ocultar parámetros concretos de la hoja de Preferencias avanzadas para obtener más información.

- 0 (predeterminado): Muestra tanto la opción de **Accesos directos** como la de **Reconexión** en la hoja Preferencias avanzadas. Por ejemplo: `CitrixWorkspaceApp.exe DisableSetting=0`.
- 1: Muestra solo la opción **Reconexión** en la hoja Preferencias avanzadas. Por ejemplo: `CitrixWorkspaceApp.exe DisableSetting=1`.
- 2: Muestra solo la opción **Accesos directos** en la hoja Preferencias avanzadas. Por ejemplo: `CitrixWorkspaceApp.exe DisableSetting=2`.
- 3: Oculta tanto la opción de **Accesos directos** y la de **Reconexión** en la hoja Preferencias avanzadas. Por ejemplo: `CitrixWorkspaceApp.exe DisableSetting=3`.

#### `EnableCEIP`

Indica su participación en el programa CEIP de mejora de la experiencia del cliente. Consulte CEIP para obtener más información.

- True (predeterminado): Participar en el programa Citrix Customer Improvement Program (CEIP). Por ejemplo: `CitrixWorkspaceApp.exe EnableCEIP=True`.
- False: Rechazar la participación en el programa Customer Experience Improvement Program (CEIP) de Citrix. Por ejemplo: `CitrixWorkspaceApp.exe EnableCEIP=False`.

#### EnableTracing

Controla la función de **Seguimiento permanente (Always-on tracing)**.

- True (valor predeterminado): Habilita la función de **Seguimiento permanente (Always-on tracing)**. Ejemplo. `CitrixWorkspaceApp.exe EnableTracing=true`.
- False: Inhabilita la función de **Seguimiento permanente (Always-on tracing)**. Por ejemplo: `CitrixWorkspaceApp.exe EnableTracing=false`.

#### CLIENT_NAME

Especifica el nombre utilizado para identificar el dispositivo de usuario en el servidor.

- `<ClientName>`: Especifica el nombre utilizado para identificar el dispositivo de usuario en el servidor. El nombre predeterminado es `%COMPUTERNAME%`. Por ejemplo: `CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%`.

#### ENABLE_DYNAMIC_CLIENT_NAME

Permite que el nombre del cliente sea el mismo que el nombre del equipo. Cuando los usuarios cambian el nombre de su equipo, el nombre de cliente también cambia.

- Sí (valor predeterminado): Permite que el nombre del cliente sea el mismo que el nombre del equipo. Por ejemplo: `CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=Yes`.
- No: No permite que el nombre del cliente sea el mismo que el nombre del equipo. Especifique un valor para la propiedad `CLIENT_NAME`. Por ejemplo: `CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=No`.

### Parámetros de autenticación

#### ENABLE_SSON

Habilita Single Sign-On cuando se instala la aplicación Workspace con el comando `/includeSSON`. Consulte Autenticación PassThrough de dominio para obtener más información.

- Sí (valor predeterminado): Indica que Single Sign-On está habilitado. Por ejemplo: `CitrixWorkspaceApp.exe ENABLE_SSON=Yes`.
- No: Indica que Single Sign-On está inhabilitado. Por ejemplo: `CitrixWorkspaceApp.exe ENABLE_SSON=No`.

#### ENABLE_KERBEROS

Especifica si HDX Engine debe usar la autenticación Kerberos, que solo se requiere cuando se habilita la autenticación Single Sign-On. Para obtener más información, consulte Autenticación PassThrough

de dominio con Kerberos.

- Sí: Indica que HDX Engine debe utilizar la autenticación Kerberos. Por ejemplo: `CitrixWorkspaceApp.exe ENABLE_KERBEROS=Yes`.
- No: Indica que HDX Engine no utiliza la autenticación Kerberos. Por ejemplo: `CitrixWorkspaceApp.exe ENABLE_KERBEROS=No`.

Además de las propiedades anteriores, también puede especificar la URL del almacén que se utiliza con la aplicación Workspace. Puede agregar hasta 10 almacenes. Utilice la siguiente propiedad para hacerlo:

```
STOREx=" storename;http[s]://servername.domain/IISLocation/discovery;[On, Off]; [storedescription]"
```

**Valores:**

- **x**: Los enteros del 0 al 9 se utilizan para identificar un almacén.
- **storename**: Nombre del almacén. Este valor debe coincidir con el nombre configurado en el servidor de StoreFront.
- **servername.domain**: El nombre de dominio completo del servidor que aloja el almacén.
- **IISLocation**: La ruta al almacén en IIS. La URL del almacén debe coincidir con la URL en el archivo de aprovisionamiento de StoreFront. La URL del almacén tiene el formato `/Citrix/store/discovery`. Para obtener la dirección URL, exporte un archivo de aprovisionamiento desde StoreFront, ábralo en el Bloc de notas y copie la dirección URL desde el elemento **Address**.
- 
- **storedescription**: Una descripción del almacén; por ejemplo, `HR App Store`.

#### Ejemplos de instalación mediante la línea de comandos

**Para especificar la URL de almacén de Citrix Gateway:**

```
CitrixWorkspaceApp.exe STORE0= HRStore;https://ag.mycompany.com##Storename; On;Store
```

Donde, **Storename** indica el nombre del almacén que debe configurarse.

> **Nota:**
>
> - La URL del almacén de Citrix Gateway debe ser la primera de la lista (parámetro STORE0).
> - En una configuración con varios almacenes, solo se permite la configuración de una URL de almacén de Citrix Gateway.
> - La URL de almacén de Citrix Gateway configurada con este método no admite los sitios de

> servicios de PNA que utilicen Citrix Gateway.
> - El parámetro "/Discovery" no es necesario cuando se especifica una URL de almacén de Citrix Gateway.

**Para instalar todos los componentes de manera silenciosa y especificar dos almacenes de aplicaciones:**

```
CitrixWorkspaceApp.exe /silent
STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;HR App
Store"
STORE1="BackUpAppStore;https://testserver.net/Citrix/MyBackupStore/discovery
;on;Backup HR App Store"
```

> **Nota:**
>
> - Es obligatorio incluir `/discovery` en la URL del almacén para que la autenticación PassThrough se lleve a cabo correctamente.
> - La URL de almacén de Citrix Gateway debe ser la primera entrada en la lista de direcciones URL configuradas de almacén.

### Restablecer la aplicación Citrix Workspace

El restablecimiento de la aplicación Citrix Workspace restaura los parámetros predeterminados.

Se restablecen estos elementos al restablecer la aplicación Citrix Workspace:

- Todas las cuentas y almacenes configurados.
- Aplicaciones entregadas por Self-Service Plug-in, sus iconos y claves de Registro.
- Asociaciones de tipos de archivo creadas por Self-Service Plug-in.
- Archivos almacenados en la caché y contraseñas guardadas.
- Parámetros del Registro por usuario.
- Instalaciones por máquina y sus parámetros del Registro.
- Parámetros del Registro de Citrix Gateway para la aplicación Citrix Workspace.

Ejecute este comando desde la interfaz de la línea de comandos para restablecer la aplicación Citrix Workspace:

```
C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.exe"-
cleanUser
```

Para el restablecimiento silencioso, use este comando:

```
C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.exe"/
silent -cleanUser
```

> **Nota:**
>
> Utilice la U mayúscula en el parámetro.

El restablecimiento de la aplicación Citrix Workspace no afecta a lo siguiente:

- Instalación de plug-ins o de la aplicación Citrix Workspace.
- Parámetros de bloqueo de ICA por máquina.
- Configuraciones de plantillas administrativas de objetos de directiva de grupo (GPO) para la aplicación Citrix Workspace.

### Desinstalación

**Usar un instalador basado en Windows:**

Puede desinstalar la aplicación Citrix Workspace para Windows desde el **Panel de control**. Para obtener más información, consulte la sección Desinstalar la aplicación Citrix Workspace para Windows.

> **Nota:**
>
> Durante la instalación de la aplicación Citrix Workspace, recibirá un mensaje para desinstalar el paquete Citrix HDX RTME. Haga clic en **Aceptar** para continuar con la desinstalación.

**Uso de la interfaz de línea de comandos:**

Puede desinstalar la aplicación Citrix Workspace desde una línea de comandos con el comando siguiente:

```
CitrixWorkspaceApp.exe /uninstall
```

Para una desinstalación silenciosa de la aplicación Citrix Workspace, ejecute el siguiente modificador de línea de comandos:

```
CitrixWorkspaceApp.exe /silent /uninstall
```

> **Nota:**
>
> El instalador de la aplicación Citrix Workspace no controla las claves del Registro relacionadas con los GPO, por lo que se conservan después de la desinstalación. Si encuentra alguna entrada, actualícelas mediante `gpedit` o elimínelas manualmente.

## Implementación

March 10, 2023

Puede implementar la aplicación Citrix Workspace con los siguientes métodos:

- Use Active Directory y los scripts de inicio de ejemplo para implementar la aplicación Citrix Workspace para Windows. Para obtener más información acerca de Active Directory, consulte Usar Active Directory y scripts de ejemplo.
- Antes de iniciar Workspace para Web, instale la aplicación Workspace para Windows. Para obtener más información, consulte Usar Workspace para Web.
- Utilice una herramienta ESD (Electronic Software Distribution) como Microsoft System Center Configuration Manager 2012 R2. Para obtener más información, consulte Usar System Center Configuration Manager 2012 R2.
- Use Microsoft Endpoint Manager (Intune). Para obtener más información, consulte Implementar la aplicación Citrix Workspace en Microsoft Endpoint Manager (Intune).

### Usar Active Directory y scripts de ejemplo

Se pueden usar los scripts de directiva de grupo de Active Directory para implementar la aplicación Citrix Workspace en función de la estructura de su organización. Citrix recomienda usar los scripts en lugar de extraer los archivos MSI. Para obtener información general acerca de los scripts de inicio, consulte la documentación de Microsoft.

**Para usar los scripts con Active Directory:**

1. Cree la unidad organizativa (UO) para cada script.
2. Cree un objeto de directiva de grupo (GPO) para la unidad organizativa recién creada.

Para obtener información sobre cómo crear una unidad organizativa en Azure Active Directory, consulte Cree una unidad organizativa (OU) en un dominio administrado de Azure Active Directory Domain Services.

#### Modificar scripts

Modifique estos parámetros de los scripts en la sección del encabezado de cada archivo:

- **Current Version of package (Versión actual del paquete):** El número de versión especificado se valida y, si no existe, se lleva a cabo la implementación. Por ejemplo, configure `DesiredVersion= 3.3.0.XXXX` para que coincida exactamente con la versión especificada. Por ejemplo, si especifica la versión parcial 3.3.0, esa versión coincidirá con cualquier versión que contenga ese prefijo (3.3.0.1111, 3.3.0.7777 y así sucesivamente).
- **Package Location/Deployment directory (Ubicación del paquete/directorio de distribución):** Especifica el recurso compartido de red que contiene los paquetes del instalador de la aplicación Citrix Workspace y no se autentica mediante el script. La carpeta compartida debe tener permisos de lectura para todos (EVERYONE).
- **Script Logging Directory (Directorio de registros del script):** El recurso compartido de la red donde se copian los registros de instalación y los que el script no autenticó. La carpeta compartida debe tener permisos de lectura y escritura para todos (EVERYONE).

- **Package Installer Command Line Options (Opciones de línea de comandos del instalador):** Estas opciones de línea de comandos se envían al instalador. Para obtener información sobre la sintaxis de la línea de comandos, consulte Usar parámetros de línea de comandos.

### Scripts

El instalador de la aplicación Citrix Workspace incluye scripts de ejemplo por equipos y por usuarios para instalar y desinstalar dicha aplicación. Los scripts se encuentran en la página Descargas de la aplicación Citrix Workspace para Windows.

| Tipo de implementación | Para implementar | Para quitar |
|---|---|---|
| Por equipo | CheckAndDeployWorkspaceP .bat | CheckAndRemoveWorkspacePerMachineS .bat |
| Por usuario | CheckAndDeployWorkspacePerUser.bat | CheckAndRemoveWorkspacePerUserLogo .bat |

**Para agregar los scripts de inicio:**

1. Abra la Consola de administración de directivas de grupo.
2. Seleccione **Configuración del equipo** o **Configuración del usuario** > **Directivas** > **Configuración de Windows** > **Scripts**.
3. En el panel derecho de la Consola de administración de directivas de grupo, seleccione **Inicio de sesión**.
4. Seleccione **Mostrar archivos**, copie el script apropiado en la carpeta que se muestra y cierre el cuadro de diálogo.
5. En el menú **Propiedades**, haga clic en **Agregar** y use la opción **Examinar** para buscar y agregar los scripts recientemente creados.

**Para implementar la aplicación Citrix Workspace para Windows:**

1. Mueva los dispositivos de usuario asignados para recibir esta implementación a la unidad organizativa creada.
2. Reinicie el dispositivo de usuario e inicie sesión.
3. Verifique que el paquete recién instalado esté listado en **Programa y características**.

**Para quitar la aplicación Citrix Workspace para Windows:**

1. Mueva los dispositivos de usuario que quiera quitar a la unidad organizativa que creó.
2. Reinicie el dispositivo de usuario e inicie sesión.
3. Verifique que el paquete recién instalado no aparezca en **Programas y características**.

### Usar Workspace para Web

Los espacios de trabajo para la web le permiten acceder a almacenes de StoreFront a través de un explorador web mediante una página web.

Antes de conectarse a una aplicación desde un explorador web, haga lo siguiente:

1. Instale la aplicación Citrix Workspace para Windows.
2. Implementar la aplicación Citrix Workspace desde Workspace para Web

Si Workspace para Web detecta que no hay una versión compatible de la aplicación Citrix Workspace, aparece un mensaje. El mensaje muestra que debe descargar e instalar la aplicación Citrix Workspace para Windows.

> **Nota:**
>
> Los espacios de trabajo para la web no admiten la detección de cuentas basada en direcciones de correo electrónico.

Use la siguiente configuración para que solo se pida la dirección del servidor.

1. Descargue `CitrixWorkspaceApp.exe` en el equipo local.
2. Cambie el nombre de `CitrixWorkspaceApp.exe` a `CitrixWorkspaceAppWeb.exe`.
3. Distribuya el ejecutable con el nuevo nombre con su método de distribución habitual. Si usa StoreFront, consulte Configurar StoreFront mediante los archivos de configuración en la documentación de StoreFront.

### Usar System Center Configuration Manager 2012 R2

Puede usar Microsoft System Center Configuration Manager (SCCM) para implementar la aplicación Citrix Workspace.

Puede implementar la aplicación Citrix Workspace con SCCM mediante las cuatro partes siguientes:

1. Agregar la aplicación Citrix Workspace a la implementación SCCM
2. Agregar puntos de distribución
3. Implementar la aplicación Citrix Workspace en el centro de software
4. Crear colecciones de dispositivos

#### Agregar la aplicación Citrix Workspace a la implementación SCCM

1. Copie la carpeta de instalación de la aplicación Citrix Workspace descargada a una carpeta en el servidor de Configuration Manager e inicie la consola de Configuration Manager.
2. Seleccione **Biblioteca de Software** > **Administración de aplicaciones**. Haga clic con el botón secundario en **Aplicación** y haga clic en **Crear aplicación**.
   Se abrirá el Asistente para crear aplicaciones.

3. En el panel **General**, haga clic en **Especificar manualmente la información de la aplicación** y, a continuación, haga clic en **Siguiente**.
4. En el panel **Información general**, especifique la información de la aplicación, como, por ejemplo, el **nombre**, el **fabricante** o la **versión de software**.
5. En el asistente **Catálogo de aplicaciones**, especifique información adicional, como el idioma, el nombre de la aplicación o la categoría de usuario, y haga clic en **Siguiente**.

   > **Nota:**
   >
   > Los usuarios pueden ver la información que especifique aquí.

6. En el panel **Tipo de implementación**, haga clic en **Agregar** para configurar el tipo de implementación para la instalación de la aplicación Citrix Workspace.

   Aparecerá el Asistente para crear tipos de implementación.

7. En el panel **General**: Establezca el tipo de implementación en el valor Windows Installer (archivo *.msi), seleccione **Especificar manualmente la información del tipo de implementación** y haga clic en **Siguiente**.
8. En el panel **Información General**, especifique los detalles del tipo de implementación (por ejemplo, Implementación de Workspace) y haga clic en **Siguiente**.
9. En el panel **Contenido**:
   a) Suministre la ruta donde se encuentra el archivo de instalación de la aplicación Citrix Workspace. Por ejemplo: Herramientas en el servidor SCCM.
   b) Especifique el **programa de instalación** como uno de los siguientes:
      - `CitrixWorkspaceApp.exe /silent` para establecer la instalación silenciosa como instalación predeterminada.
      - `CitrixWorkspaceApp.exe /silent /includeSSON` para habilitar el PassThrough de dominio
      - `CitrixWorkspaceApp.exe /silent SELFSERVICEMODE=false` para instalar la aplicación Citrix Workspace en un modo que no sea de autoservicio.

   c) Especifique **Programa de desinstalación** como `CitrixWorkspaceApp.exe /silent /uninstall` (para habilitar la desinstalación a través de SCCM).
10. En el panel **Método de detección**, seleccione **Configurar reglas para detectar la presencia de este tipo de implementación** y haga clic en **Agregar cláusula**.
    Aparece el cuadro de diálogo Regla de actualización.
    - Establezca **Tipo de configuración** en “Sistema de archivos”.
    - En **Especificar el archivo o la carpeta para detectar esta aplicación**, establezca las siguientes opciones:
      - **Tipo**: En el menú desplegable, seleccione **Archivo**.

- **Ruta:** `%ProgramFiles(x86)%\Citrix\ICA Client\Receiver\`
- **Nombre de archivo o carpeta:** `receiver.exe`
- **Propiedad:** En el menú desplegable, seleccione **Versión**.
- **Operador:** En el menú desplegable, seleccione **Mayor o igual que**.
- **Valor**: Escriba el número de versión actual de la aplicación Citrix Workspace.

> **Nota:**
>
> Esta combinación de reglas también es aplicable a actualizaciones de la aplicación Citrix Workspace para Windows.

11. En el panel **Experiencia del usuario**, establezca:
    - **Comportamiento de instalación:** Instalar para el sistema.
    - **Requisito de inicio de sesión**: Si un usuario inició sesión.
    - **Visibilidad del programa de instalación**: Normal

    Haga clic en **Siguiente**.

> **Nota:**
>
> No especifique requisitos ni dependencias para este tipo de implementación.

12. En el panel **Resumen**, verifique los parámetros de este tipo de implementación. Haga clic en **Siguiente**.

    Aparecerá un mensaje indicando que la conexión tuvo lugar.

13. En el **panel Finalización**, aparece listado un nuevo tipo de implementación (Implementación de Workspace) en **Tipos de implementación**.
14. Haga clic en **Siguiente** y **Cerrar**.

#### Agregar puntos de distribución

1. Haga clic con el botón secundario en la aplicación Citrix Workspace desde la consola de **Configuration Manager** y seleccione **Distribuir contenido**.

   Aparecerá el asistente para distribuir contenido.

2. En el panel "Distribución de contenido", haga clic en **Agregar > Puntos de distribución**.

   Aparecerá el cuadro de diálogo para agregar puntos de distribución.

3. Vaya al servidor de SCCM donde está disponible el contenido y haga clic en **Aceptar**.

   En el panel "Finalización", se muestra un mensaje indicando que la operación es correcta.

4. Haga clic en **Cerrar**.

**Implementar la aplicación Citrix Workspace en el centro de software**

1. Haga clic con el botón secundario en la aplicación Citrix Workspace en la consola de Configuration Manager y seleccione **Implementar**.

   Aparece el asistente para implementar software.

2. Seleccione **Examinar** y vaya a la colección (puede ser "Recopilación de dispositivo" o "Recopilación de usuario") donde la aplicación va a implementarse y haga clic en **Siguiente**.

3. En el panel **Configuración de implementación**, establezca **Acción** en "Instalar" y **Propósito** en "Requerido" (permite la instalación sin supervisión). Haga clic en **Siguiente**.

4. En el panel **Programación**, especifique la programación para implementar el software en los dispositivos de destino.

5. En el panel **Experiencia del usuario**, establezca el comportamiento de las **Notificaciones de usuario**; seleccione **Confirmar cambios dentro de la fecha límite o en una ventana de mantenimiento (reinicio necesario)** y haga clic en **Siguiente** para completar el asistente para implementar software.

En el panel **Finalización**, se muestra un mensaje que indica que la operación se realizó correctamente.

Reinicie los dispositivos de punto final de destino (requerido solo para iniciar la instalación inmediatamente).

En los dispositivos de punto final, la aplicación Citrix Workspace está visible en el Centro de software, en **Software disponible**. La instalación se activa automáticamente en función de la programación configurada. También puede programarla o llevar a cabo la instalación a demanda. Una vez comenzada la instalación, se muestra el estado de esta en el **Centro de software**.

**Crear colecciones de dispositivos**

1. Abra la consola de **Configuration Manager** y haga clic en **Activos y compatibilidad** > **Resumen** > **Dispositivos**.

2. Haga clic con el botón secundario en **Recopilaciones de dispositivos** y seleccione **Crear recopilación de dispositivos**.

   Se abrirá el asistente para **crear recopilaciones de dispositivos**.

3. En el panel **General**, escriba el **Nombre** del dispositivo y haga clic en **Examinar** para seleccionar la recopilación de restricción.

   Esto determina el ámbito de los dispositivos, que puede ser una de las **recopilaciones de dispositivos** predeterminadas creadas por SCCM.
   Haga clic en **Siguiente**.

4. En el panel **Reglas de pertenencia**, haga clic en **Agregar regla** para filtrar los dispositivos.

   Aparecerá el asistente para **crear reglas de pertenencia directa**.

   - En el panel **Buscar recursos**, seleccione el **Nombre del atributo** en función de los dispositivos que quiere filtrar y suministre el valor del Nombre del atributo para seleccionar los dispositivos.

5. Haga clic en **Siguiente**. En el panel Seleccionar recursos, seleccione los dispositivos que deben formar parte de la colección de dispositivos.

   En el panel Finalización, se muestra un mensaje que indica que la operación se realizó correctamente.

6. Haga clic en **Cerrar**.

7. En el panel Reglas de pertenencia, aparecerá una nueva regla. Haga clic en Siguiente.

8. En el panel Finalización, se muestra un mensaje que indica que la operación se realizó correctamente. Haga clic en **Cerrar** para completar el Asistente para **crear una recopilación de dispositivos**.

   La nueva colección de dispositivos aparece en **Recopilaciones de dispositivos**. La nueva recopilación de dispositivos forma parte de las Recopilaciones de dispositivos al buscar en el **asistente para implementar software**.

> **Nota:**
>
> Es posible que la configuración de la aplicación Citrix Workspace mediante SCCM falle cuando el atributo **MSIRESTARTMANAGERCONTROL** se establece en **False**.
> Según nuestros análisis, la aplicación Citrix Workspace para Windows no es la causa de este fallo. Además, la implementación puede ser correcta en el siguiente intento.

### Implementar la aplicación Citrix Workspace en Microsoft Endpoint Manager (Intune)

Para implementar la aplicación Citrix Workspace (aplicación Win 32 nativa) en Microsoft Endpoint Manager (Intune), haga lo siguiente:

1. Cree estas carpetas:

   - Una carpeta para almacenar todos los archivos de origen necesarios para la instalación. Por ejemplo: `C:\CitrixWorkspace_Executable`.
   - Una carpeta para el archivo de salida. Los archivos de salida están en el archivo `.intunewin`. Por ejemplo: `C:\Intune_CitrixWorkspaceApp`.
   - Una carpeta para la herramienta Microsoft Win32 Content Prep. Por ejemplo: `C:\Intune_WinAppTool`. Esta herramienta ayuda a convertir los archivos de instalación al

formato `.intunewin`. Puede descargar la herramienta de empaquetado en Microsoft-Win32-Content-Prep-Tool.

2. Convierta todos los archivos de origen que se necesitan para la instalación en un archivo `.intunewin`:

   a) Inicie el símbolo del sistema y vaya a la carpeta donde existe Microsoft Win32 Content Prep Tool. Por ejemplo: `C:\Intune_WinAppTool`.
   b) Ejecute el comando `IntuneWinAppUtil.exe`.
   c) En el mensaje, introduzca esta información:
      - **Source folder**: `C:\CitrixWorkspace_Executable`
      - **Setup file**: `CitrixWorkspaceApp.exe`
      - **Output folder**: `C:\Intune_CitrixWorkspaceApp`

      Se crea el archivo `.intunewin`.

3. Agregue el paquete a Microsoft Endpoint Manager (Intune):

   a) Abra la consola de Microsoft Endpoint Manager (Intune): `https://endpoint.microsoft.com/##home`.

      > **Nota:**
      >
      > Esta instrucción solo se puede realizar en `https://endpoint.microsoft.com/##home`. También puede agregar el paquete a través de `https://portal.azure.com`.

   b) Haga clic en **Apps** > **Windows app** y, a continuación, en **+Add**.
   c) Seleccione **Windows app (Win 32)** en la lista desplegable **App type**.
   d) Haga clic en **App package file**, busque el archivo CitrixWorkspaceApp.intunewin y, a continuación, haga clic en **OK**.
   e) Haga clic en **App information** y complete la información obligatoria (Name, Description y Publisher) y, a continuación, haga clic en **OK**.
   f) Haga clic en **Program**, introduzca esta información y haga clic en **OK**:
      - Comando de instalación: `CitrixWorkspaceApp.exe /silent`
      - Comando de desinstalación: `CitrixWorkspaceApp.exe /uninstall`
      - Comportamiento de instalación: System
   g) Haga clic en **Requirement**, introduzca la información requerida y, a continuación, haga clic en **OK**.

      > **Nota:**

> Seleccione x64 y x32 en la lista Operating System Architecture. La versión del sistema operativo puede ser cualquiera con Win 1607 o una versión posterior.

h) Haga clic en **Detection rules**, seleccione **Manually configure detection rules** bajo **Rules format** y, a continuación, haga clic en **OK**.

i) Haga clic en **Add**, seleccione el tipo de regla necesario en **Rule type** y, a continuación, haga clic en **OK**.

- Si **Rule type** es **File**, la ruta puede ser, por ejemplo, `C:\Program Files (x86)\Citrix\ICA Client\wfica32.exe`.
- Si **Rule type** es **Registry**, introduzca `HKEY_CURRENT_USER\Software\Citrix` como **Path** y **Key exists** como **Detection method**.

j) Haga clic en **Return codes**, compruebe si los códigos de devolución predeterminados son válidos y haga clic en **OK**.

k) Haga clic en **Add** para agregar la aplicación a Intune.

4. Compruebe si la implementación se ha realizado correctamente:

a) Haga clic en **Home** > **Apps** > **Windows**.

b) Haga clic en **Device install status**.

El estado del dispositivo muestra la cantidad de dispositivos en los que está instalada la aplicación Citrix Workspace.

## Actualización

January 24, 2023

### Actualización manual

Si ya instaló la aplicación Citrix Workspace para Windows, descargue e instale la versión más reciente de la aplicación desde la página Descargas de Citrix. Para obtener información sobre la instalación, consulte Instalación y desinstalación.

### Actualización automática

Cuando hay una nueva versión disponible de la aplicación Citrix Workspace, Citrix envía una actualización al sistema que tiene instalada la aplicación Citrix Workspace.

**Nota:**

- Si configuró un proxy SSL interceptor de salida, agregue una excepción al servicio de firma de actualización automática de Workspace `https://citrixupdates.cloud.com/` y a la ubicación de descarga `https://downloadplugins.citrix.com/` para recibir actualizaciones de Citrix.
- El sistema debe tener una conexión a Internet para recibir actualizaciones.
- De forma predeterminada, las actualizaciones de Citrix Workspace están inhabilitadas en el VDA. Esto incluye máquinas de servidor multiusuario RDS, máquinas VDI y máquinas de acceso con Remote PC.
- Las actualizaciones de Citrix Workspace están inhabilitadas en máquinas donde esté instalado Desktop Lock.
- Los usuarios de Workspace para Web no pueden descargar automáticamente la directiva de StoreFront.
- La función Actualizaciones de Citrix Workspace solo se puede limitar a las actualizaciones LTSR.
- Citrix HDX RTME para Windows se incluye en Actualizaciones de Citrix Workspace. Aparece una notificación cuando hay actualizaciones disponibles de HDX RTME tanto en la versión LTSR como en la versión Current Release de la aplicación Citrix Workspace.
- A partir de la versión 2105, se modifican las rutas de registros de Actualizaciones de Citrix Workspace. Los registros de Actualizaciones de Workspace están en C:\Archivos de programa (x86)\Citrix\Logs. Para obtener información sobre la captura de registros, consulte la sección Recopilación de registros.
- Los usuarios que no sean administradores pueden actualizar la aplicación Citrix Workspace en instancias instaladas por un administrador. Para ello, haga clic con el botón secundario en el icono de la aplicación Citrix Workspace, en el área de notificaciones, y seleccione **Buscar actualizaciones**. La opción **Buscar actualizaciones** está disponible tanto en las instancias instaladas por el usuario como en las instancias instaladas por el administrador de la aplicación Citrix Workspace.
- También puede realizar la actualización automática cuando están habilitadas la detección del protocolo de detección automática de proxies web (WPAD) y la configuración automática de proxy (PAC). Esto no se admite cuando el proxy requiere credenciales para la autenticación.
- Si se agrega un conjunto de cifrado que no sea EDCHE, Citrix Workspace no puede contactar con el servidor de actualización automática de Citrix, y aparece este error durante la actualización automática:

> **No se puede conectar con el servidor**

Reinicie la aplicación Citrix Workspace para Windows tras una actualización manual o automática.

Puede comprobar la versión actual de la aplicación Citrix Workspace instalada en su dispositivo a través de **Preferencias avanzadas** o consultar el registro **DisplayVersion** desde la ubicación `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\CitrixOnlinePluginPackWeb`.

Para ver la versión en **Preferencias avanzadas**:

1. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace situado en el área de notificaciones.
2. Seleccione **Preferencias avanzadas**.

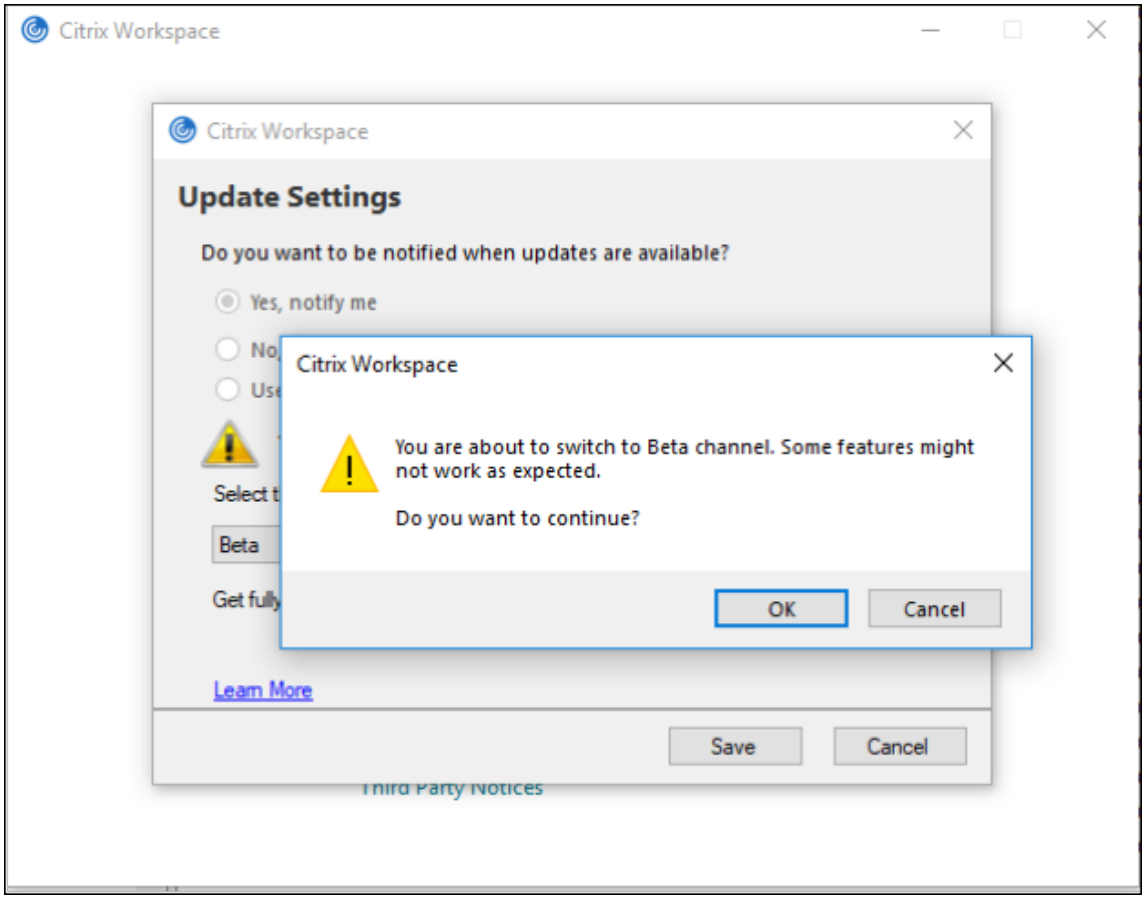
   La versión de la aplicación Citrix Workspace aparece en la sección **Acerca de**.

### Instalar el programa Beta de la aplicación Citrix Workspace

Recibirá una notificación de actualización cuando la Citrix Workspace se haya configurado para obtener actualizaciones automáticas. Para instalar la compilación Beta en el sistema, siga estos pasos:

1. Abra la aplicación Citrix Workspace desde el área de notificaciones.
2. Vaya a **Preferencias avanzadas** > **Actualizaciones de Citrix Workspace**.
3. Seleccione **Beta** en la lista desplegable cuando la compilación Beta esté disponible y haga clic en **Guardar**.
   Aparecerá una ventana de notificación.




4. Haga clic en **Aceptar** para actualizar su versión a la versión Beta.

Para cambiar de una compilación Beta a una compilación pública, siga estos pasos:

1. Abra la aplicación Citrix Workspace desde el área de notificaciones.
2. Vaya a **Preferencias avanzadas** > **Actualizaciones de Citrix Workspace**.
3. En la pantalla **Parámetros de actualización** , seleccione **Público** en la lista desplegable “Canal de actualización” y haga clic en **Guardar**.

> **Nota:**
>
> - Si hay nuevas actualizaciones disponibles, aparece una notificación de actualización automática.
> - Las compilaciones beta están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción y para compartir comentarios. Citrix no acepta casos de asistencia de compilaciones beta, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

#### Función de actualización automática de la aplicación Citrix Workspace en VDA

A partir de la versión 2209 de la aplicación Citrix Workspace para Windows, puede habilitar la función de actualización automática en VDA mediante la creación de este valor del Registro:

En una máquina de 32 bits:

- Clave del Registro: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\AutoUpdate
- Valor del Registro: AllowAutoUpdateOnVDA
- Tipo de Registro: REG_SZ
- Datos del Registro: True

En una máquina de 64 bits:

- Clave del Registro: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\AutoUpdate
- Valor del Registro: AllowAutoUpdateOnVDA
- Tipo de Registro: REG_SZ
- Datos del Registro: True

### Control de versiones con actualización automática

Ahora, los administradores pueden administrar la versión de las actualizaciones automáticas de los dispositivos de la organización.

Los administradores pueden controlar la versión estableciéndola en la propiedad maximumAllowed-Version de Global App Config Service.

Ejemplo de archivo JSON en Global App Config Service:

```
"AutoUpdate": {


"userOverride": false,

"AutoUpdatePluginsSettings": [

    {


    "pluginSettings":

{
        "upgradeToLatest": false,
        "maximumAllowedVersion": "22.9.0.3934",                }


,
```

```
19
20      "pluginName": "WorkspaceApp",
21
22      "pluginId": "1CDF566D-B2C7-47F-6283C862E1D6"
23
24     }
25
26
27  <!--NeedCopy-->
```

Cuando se establece la versión, la aplicación Citrix Workspace del dispositivo del usuario se actualiza automáticamente con la versión especificada en la propiedad maximumAllowedVersion.

> **Notas:**
>
> - Para efectuar el control de versiones de las actualizaciones automáticas, el parámetro upgradeToLatest de Global App Config Service debe estar establecido en false. Si se establece en verdadero, se ignorará la propiedad maximumAllowedVersion.
> - No modifique pluginId, ya que está asignado a la aplicación Citrix Workspace.
> - Si el administrador no ha configurado la versión en Global App Config Service, la aplicación Citrix Workspace se actualiza a la versión disponible más reciente de forma predeterminada.

### Configuración avanzada para actualizaciones automáticas (Actualizaciones de Citrix Workspace)

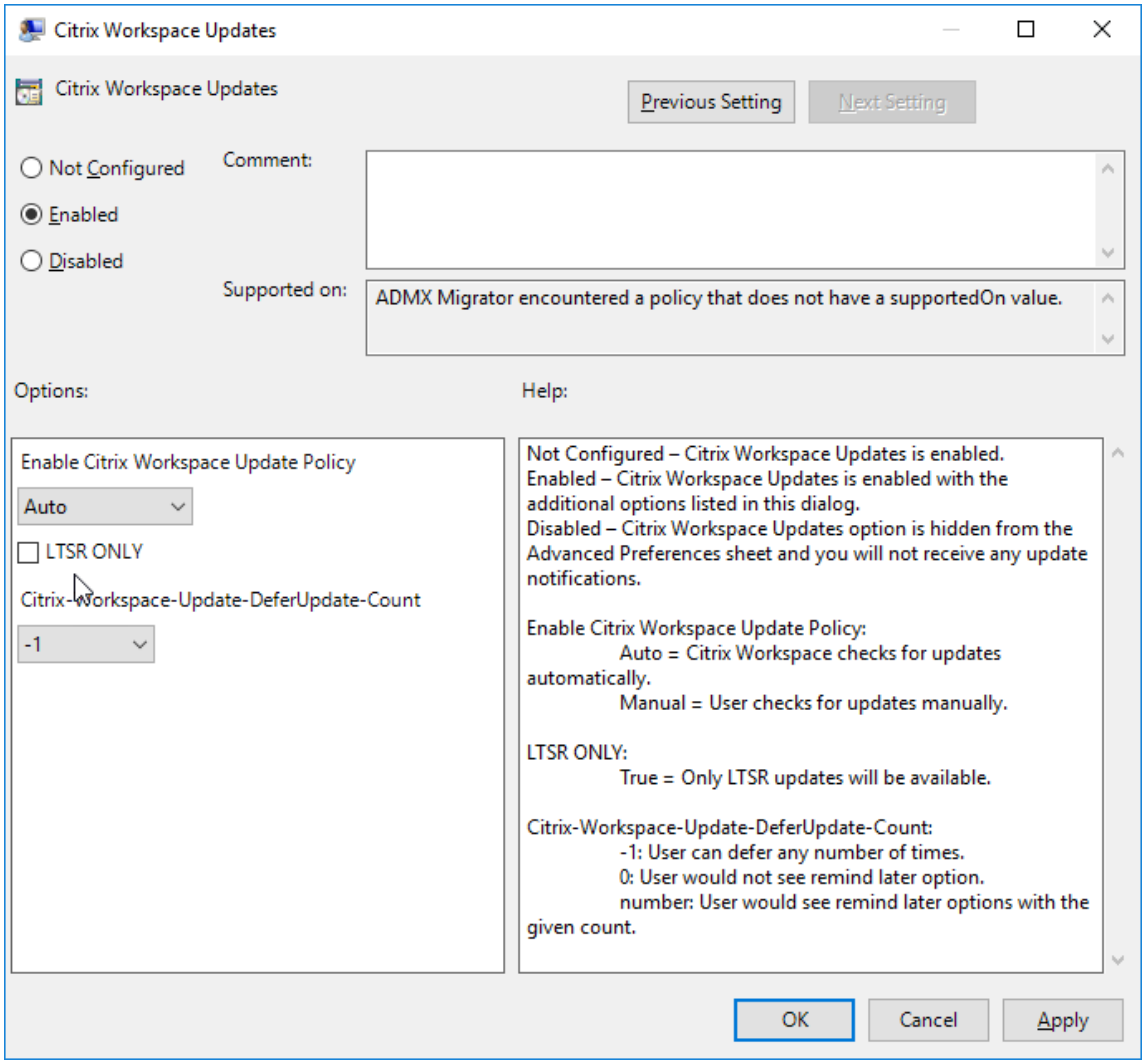
Puede configurar Actualizaciones de Citrix Workspace con estos métodos:

1. Plantilla administrativa de objetos de directiva de grupo (GPO)
2. Interfaz de la línea de comandos
3. Interfaz gráfica (GUI)
4. StoreFront

#### Configurar Actualizaciones de Citrix Workspace con la plantilla administrativa de objeto de directiva de grupo

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc y vaya al nodo Configuración del equipo.
2. Vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Actualizaciones de Workspace**.




3. **Habilitar o inhabilitar actualizaciones**. Seleccione **Habilitado** o **Inhabilitado** para habilitar o inhabilitar Actualizaciones de Workspace.

   > **Nota:**
   >
   > Si marca **Inhabilitado**, no se le notificará de nuevas actualizaciones disponibles. La opción **Inhabilitada** también oculta la opción Actualizaciones de Citrix Workspace en la hoja Preferencias avanzadas.

4. **Notificación de actualización**. Cuando haya una actualización disponible, puede optar por recibir una notificación automática o comprobarlo manualmente. Una vez habilitadas las actualizaciones de Workspace, seleccione una de las opciones siguientes en la lista desplegable **Directiva para habilitar la actualización de Citrix Workspace**:

   - Auto: Se le notificará cuando haya una actualización disponible (predeterminado).
   - Manual: No se le notificará cuando haya actualizaciones disponibles. Compruebe manualmente si hay actualizaciones.

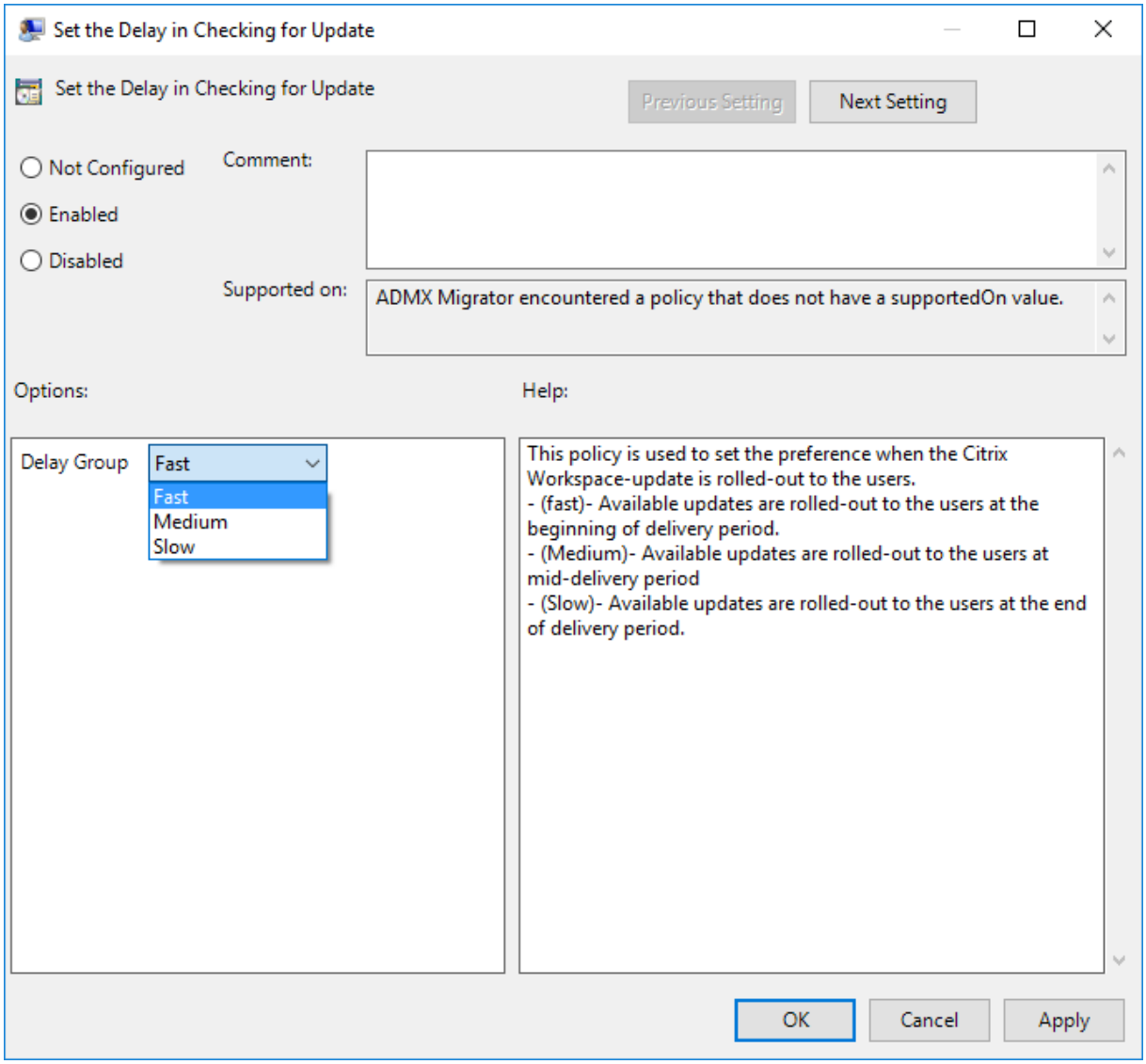
5. Seleccione **SOLO LTSR** para obtener las actualizaciones para LTSR solamente.
6. En la lista desplegable **Citrix-Workspace-Update-DeferUpdate-Count**, seleccione un valor entre -1 y 30:
    - Si el valor es 0, no aparece la opción **Recordármelo más tarde**. El mensaje **Actualización disponible** se muestra tras cada comprobación automática periódica de actualizaciones.
    - Si el valor es -1, aparece la opción **Recordármelo más tarde** con el mensaje **Actualización disponible**. Puede aplazar la notificación de actualizaciones las veces que quiera.
    - Un valor entre 1 y 30 define la cantidad de veces que debe aparecer la opción **Recordármelo más tarde** con el mensaje **Actualización disponible**. Puede aplazar la notificación de actualizaciones en función del valor definido en este campo. Sin embargo, el mensaje **Actualización disponible** sigue apareciendo, pero sin la opción **Recordármelo más tarde**.

#### Configurar la demora en la comprobación de actualizaciones

Cuando hay disponible una nueva versión de la aplicación Workspace, Citrix implanta la actualización durante un período de entrega específico. Con esta propiedad, puede controlar el momento del período de entrega en que puede recibir la actualización.

Para configurar el período de entrega, ejecute `gpedit.msc` para iniciar la plantilla administrativa de objeto de directiva de grupo. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Definir demora para comprobar actualizaciones**.




**Habilítela** y, en el menú desplegable **Demorar grupo**, seleccione una de estas opciones:

- Fast (Rápido): La implantación de la actualización tiene lugar al comienzo del período de entrega.
- Medium (Medio): La implantación de la actualización tiene lugar hacia la mitad del período de entrega.
- Slow (Lento): La implantación de la actualización tiene lugar al final del período de entrega.

> **Nota:**
>
> Si marca **Inhabilitada**, no se le notificará de actualizaciones disponibles. La opción **Inhabilitada** también oculta la opción Actualizaciones de Citrix Workspace en la hoja Preferencias avanzadas.

### Configurar Actualizaciones de Citrix Workspace mediante la interfaz de línea de comandos

#### Especificando parámetros de línea de comandos al instalar la aplicación Workspace:

Puede configurar las actualizaciones de Workspace especificando parámetros de línea de comandos durante la instalación de la aplicación Citrix Workspace. Consulte Parámetros de instalación para obtener más información.

#### Mediante parámetros de línea de comandos después de instalar la aplicación Citrix Workspace:

Actualizaciones de Citrix Workspace se puede configurar después de instalar la aplicación Citrix Workspace para Windows. Vaya a la ubicación de `CitrixReceiverUpdater.exe` mediante la línea de comandos de Windows.

Por regla general, CitrixReceiverUpdater.exe se encuentra en `CitrixWorkspaceInstallLocation\Citrix\Ica Client\Receiver`. Puede ejecutar el binario `CitrixReceiverUpdater.exe` junto con los parámetros de línea de comandos que se indican en la sección Parámetros de instalación.

Por ejemplo:

```
CitrixReceiverUpdater.exe /AutoUpdateCheck=auto /AutoUpdateStream=Current /DeferUpdateCount=-1 /AURolloutPriority=fast
```

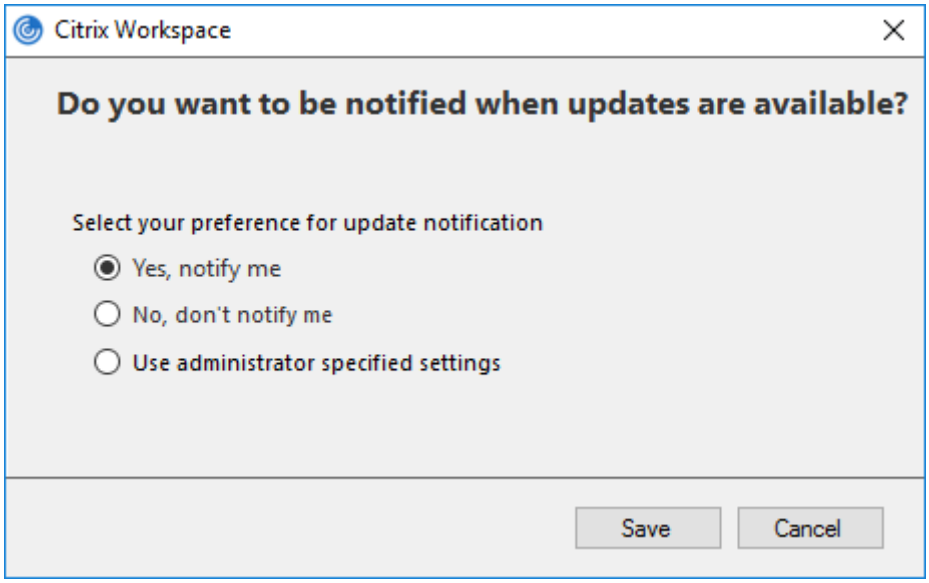
> **Nota:**
>
> `/AutoUpdateCheck` es un parámetro obligatorio que debe definir para configurar otros parámetros como `/AutoUpdateStream`, `/DeferUpdateCount` o `/AURolloutPriority`.

### Configurar Actualizaciones de Citrix Workspace mediante la interfaz gráfica de usuario

Un usuario individual puede supeditar el parámetro **Actualizaciones de Citrix Workspace** desde el cuadro de diálogo **Preferencias avanzadas**. Se trata de una configuración específica de usuario y los parámetros se aplican solamente al usuario actual.

1. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace situado en el área de notificaciones.
2. Seleccione **Preferencias avanzadas** > **Actualizaciones de Citrix Workspace**.
3. Seleccione la preferencia de notificación y haga clic en **Guardar**.




> **Nota:**
>
> Puede ocultar una parte o toda la hoja de Preferencias avanzadas disponible en el icono de la aplicación Citrix Workspace. Para obtener más información, consulte la sección Hoja de Preferencias avanzadas.

**Configurar Actualizaciones de Citrix Workspace mediante StoreFront**

1. Utilice un editor de texto para abrir el archivo `web.config`, que normalmente se encuentra en `C:\inetpub\wwwroot\Citrix\Roaming directory`.
2. Localice el elemento de la cuenta de usuario en el archivo (Store es el nombre de cuenta de la implementación)

   Por ejemplo: `<account id=... name="Store">`

   Antes de la etiqueta `</account>`, vaya a las propiedades de esa cuenta de usuario:

   ```
   <properties>
          <clear/>
    </properties>
    <!--NeedCopy-->
   ```

3. Agregue la etiqueta de actualización automática después de la etiqueta *<clear />*.

   ```
   <account>

       <clear />

       <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
           F84Store"
   ```

```
6
7       description="" published="true" updaterType="Citrix"
            remoteAccessType="None">
8
9       <annotatedServices>
10
11        <clear />
12
13        <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
14
15          <metadata>
16
17            <plugins>
18
19              <clear />
20
21            </plugins>
22
23            <trustSettings>
24
25              <clear />
26
27            </trustSettings>
28
29            <properties>
30
31              <property name="Auto-Update-Check" value="auto" />
32
33              <property name="Auto-Update-DeferUpdate-Count" value
                    ="1" />
34
35                    <property name="Auto-Update-LTSR-Only" value
                        ="FALSE" />
36
37              <property name="Auto-Update-Rollout-Priority" value=
                    "fast" />
38
39                  </properties>
40
41          </metadata>
42
43        </annotatedServiceRecord>
44
45      </annotatedServices>
46
```

```
47        <metadata>
48
49          <plugins>
50
51            <clear />
52
53          </plugins>
54
55          <trustSettings>
56
57            <clear />
58
59          </trustSettings>
60
61          <properties>
62
63            <clear />
64
65          </properties>
66
67        </metadata>
68
69      </account>
70
71  <!--NeedCopy-->
```

El significado de las propiedades y sus posibles valores se detallan a continuación:

- **Auto-update-Check:** Indica que la aplicación Citrix Workspace detecta automáticamente cuándo hay una actualización disponible.
  - Auto (predeterminado): Comprueba y realiza las actualizaciones automáticamente
  - Manual: Las actualizaciones solo se obtienen cuando el usuario realiza una solicitud de comprobación desde el menú de la bandeja del sistema de la aplicación Citrix Workspace,
  - Disabled: No se realizan comprobaciones de actualizaciones.
- **Auto-update-LTSR-Only:** Indica que la actualización es solamente para LTSR.
  - True: El programa de actualización ignora las actualizaciones que no estén marcadas como válidas para LTSR. Solo se tienen en cuenta las actualizaciones LTSR.
  - False (predeterminado) : El programa de actualización solo considera las actualizaciones por stream actuales.
- **Auto-Update-Rollout-Priority**: Indica el período de entrega en el que puede recibir la actualización.

  - Fast: Las actualizaciones se envían a los usuarios hacia el comienzo del período de entrega.
  - Medium: Las actualizaciones se implementan hacia la mitad del período de entrega.
  - Slow: Las actualizaciones se implementan al final del período de entrega.

- **Auto-update-DeferUpdate-Count:** Indica el número de veces que puede aplazar las notificaciones relativas a las actualizaciones.

  > **Nota:**
  >
  > Esta configuración solo es aplicable a las actualizaciones interactivas y no cuando la función de actualización automática silenciosa está habilitada, ya que el usuario no tiene una opción para aplazar las actualizaciones.

  - -1: El usuario puede posponer la actualización cuantas veces quiera.
  - 0: El usuario no puede ver la opción de recordatorio.
  - número: El usuario puede ver las opciones de recordatorio la cantidad de veces especificada.

# Introducción

February 17, 2023

Este artículo es un documento de referencia para configurar el entorno después de instalar la aplicación Citrix Workspace.

## Almacén

Un **almacén** reúne las aplicaciones y los escritorios disponibles para un usuario en un mismo lugar. Un usuario puede tener varios almacenes y cambiar de uno a otro según sea necesario. Un administrador entrega la URL del almacén que tiene recursos y ajustes preconfigurados. Puede acceder a estos almacenes a través de la aplicación Citrix Workspace.

## Tipos de almacenes

Puede agregar los siguientes tipos de almacenes en la aplicación Citrix Workspace: Workspace, StoreFront, almacén de Citrix Gateway y almacén web personalizado.

### Workspace

Citrix Workspace es un almacén de aplicaciones de empresa basado en la nube que proporciona acceso seguro y unificado a aplicaciones, escritorios y contenido (recursos) desde cualquier lugar y en

cualquier dispositivo. Estos recursos pueden ser Citrix DaaS, aplicaciones de contenido, aplicaciones locales y móviles, aplicaciones web y SaaS y aplicaciones para explorador web. Para obtener más información, consulte Descripción general de Citrix Workspace.

#### StoreFront

StoreFront es un intuitivo almacén de aplicaciones de empresa local que combina aplicaciones y escritorios de los sitios de Citrix Virtual Apps and Desktops en un solo almacén.

Para obtener más información, consulte la documentación de StoreFront.

#### Almacén de Citrix Gateway

Configure Citrix Gateway para permitir que los usuarios se conecten desde fuera de la red interna. Por ejemplo, usuarios que se conectan desde Internet o ubicaciones remotas.

#### Almacenes web personalizados

Esta función proporciona acceso al almacén web personalizado de su organización desde la aplicación Citrix Workspace para Windows. Para usar esta función, el administrador debe agregar el dominio o el almacén web personalizado a las URL permitidas de Global App Configuration Service.

Para obtener más información sobre cómo configurar las direcciones URL de almacén web para los usuarios finales, consulte Global App Configuration Service.

Puede proporcionar la URL del almacén web personalizado en la pantalla **Agregar cuenta** de la aplicación Citrix Workspace. El almacén web personalizado se abre en la ventana de la aplicación Workspace nativa.

Para quitar el almacén web personalizado, vaya a **Cuentas** > **Agregar o quitar cuentas**, seleccione la URL del almacén web personalizado y haga clic en **Quitar**.

### Agregar URL de almacén a la aplicación Citrix Workspace

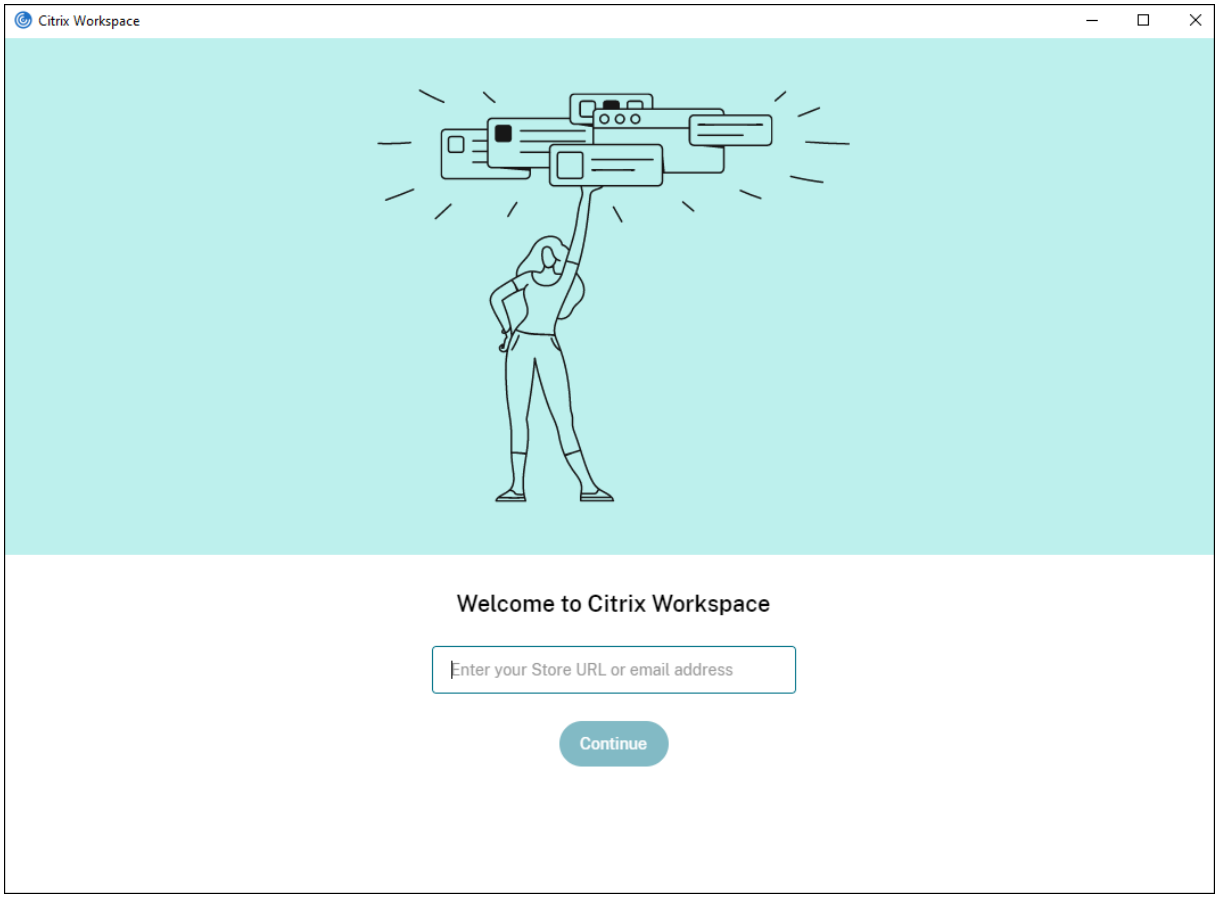
Puede hacer lo siguiente para proporcionar a los usuarios la información de cuenta que necesitan para acceder a sus escritorios y aplicaciones virtuales:

- Proporcionar información de cuenta a los usuarios para que la introduzcan manualmente
- Configurar la detección de cuentas basada en direcciones de correo electrónico
- Agregar almacén a través de la CLI
- Archivo de aprovisionamiento
- Usar la plantilla administrativa de objeto de directiva de grupo

**Proporcionar información de cuenta a los usuarios para que la introduzcan manualmente**

Tras la instalación correcta de la aplicación Citrix Workspace, aparece esta pantalla. Los usuarios deben introducir una dirección de correo electrónico o de servidor para acceder a las aplicaciones y escritorios. Cuando un usuario introduce la información de una cuenta nueva, la aplicación Citrix Workspace intenta verificar la conexión. Si la conexión puede establecerse, la aplicación Citrix Workspace solicita al usuario que inicie sesión en la cuenta.




Para permitir que los usuarios configuren sus cuentas manualmente, distribuya la información que necesitan para conectarse con sus escritorios y aplicaciones virtuales.

- Para conectarse a un almacén de Workspace, proporcione la URL de Workspace.
- Para conectarse a un almacén de StoreFront, proporcione la dirección URL de ese servidor. Por ejemplo: `https://servername.company.com`.
- Para conectarse a través de Citrix Gateway, primero determine si el usuario necesita ver todos los almacenes configurados o solo el almacén que tiene habilitado el acceso remoto para un dispositivo Citrix Gateway concreto.
  - Para presentarles todos los almacenes configurados, proporcione a sus usuarios el nombre de dominio completo de Citrix Gateway.

- Para limitar el acceso a un almacén en concreto, proporcione a sus usuarios el nombre de dominio completo de Citrix Gateway y el nombre del almacén, con el formato:

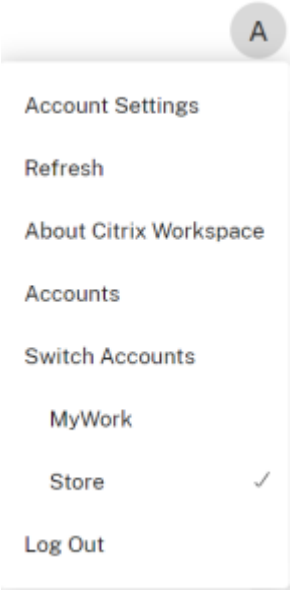
  **CitrixGatewayFQDN?MyStoreName:**

  Por ejemplo, si tiene un almacén llamado “AplicacionesVentas” con acceso remoto habilitado para servidor1.com, y un almacén llamado **AplicacionesRRHH** con acceso remoto habilitado para servidor2.com, el usuario deberá introducir:

  * servidor1.com?AplicacionesVentas para acceder a AplicacionesVentas
  * O servidor2.com?AplicacionesRRHH para acceder a **AplicacionesRRHH**.

  La función **CitrixGatewayFQDN?MyStoreName** requiere que un nuevo usuario cree una cuenta mediante una dirección URL, y no está disponible para la detección basada en direcciones de correo electrónico.

Una vez que la aplicación Workspace se haya configurado con la URL del almacén, la cuenta se puede administrar desde la opción **Cuentas** del menú de perfil.




En las máquinas cliente configuradas para la autenticación de proxy, si las credenciales de proxy no se almacenan en el **Administrador de credenciales de Windows**, aparece un mensaje de autenticación en el que se le pide que introduzca las credenciales del proxy. A continuación, la aplicación Citrix Workspace guarda las credenciales del servidor proxy en el **Administrador de credenciales de Windows**. Esto simplifica la experiencia de inicio de sesión porque no necesita guardar manualmente las credenciales en el **Administrador de credenciales de Windows** antes de acceder a la aplicación Citrix Workspace.

#### Configurar la detección de cuentas basada en direcciones de correo electrónico

Cuando se configura la aplicación Citrix Workspace para la detección de cuentas basada en direcciones de correo electrónico, los usuarios introducen su dirección de correo electrónico (en lugar de una dirección URL de servidor) durante la instalación y configuración inicial de la aplicación Citrix Workspace. La aplicación Citrix Workspace determina el dispositivo Citrix Gateway o el servidor de StoreFront asociados a la dirección de correo electrónico en función de los registros de servicios (SRV) del Sistema de nombres de dominio (DNS). A continuación, la aplicación solicita al usuario que inicie sesión para acceder a aplicaciones y escritorios virtuales.

Para configurar la detección de cuentas basada en correo electrónico para los almacenes de Citrix Workspace, consulte la sección Getting started en la documentación de Global App Configuration Service.
Para configurar la detección de cuentas basada en correo electrónico para los almacenes de Citrix StoreFront o Citrix Gateway, consulte Configuring email-based account discovery.

#### Agregar almacén a través de la CLI

Instale la aplicación Citrix Workspace para Windows como administrador desde la interfaz de línea de comandos.

Para obtener más información, consulte Lista de parámetros de la línea de comandos.

#### Proporcionar archivos de aprovisionamiento a los usuarios

StoreFront proporciona los archivos de aprovisionamiento que los usuarios pueden abrir para conectar con almacenes.

Es posible utilizar StoreFront para crear archivos de aprovisionamiento que incluyan los detalles de conexión de las cuentas. Estos archivos se ponen a disposición de los usuarios para que puedan configurar automáticamente la aplicación Citrix Workspace. Después de instalar la aplicación Citrix Workspace, los usuarios no tienen más que abrir el archivo para configurarla. Si configura sitios de Workspace para Web, los usuarios también podrán obtener los archivos de aprovisionamiento para la aplicación Citrix Workspace desde esos sitios.

Para obtener más información, consulte Para exportar archivos de aprovisionamiento del almacén para los usuarios en la documentación de StoreFront.

#### Usar la plantilla administrativa de objeto de directiva de grupo

Para agregar o especificar un Citrix StoreFront o Gateway mediante la plantilla administrativa de objetos de directiva de grupo:

1. Ejecute `gpedit.msc` para abrir la plantilla administrativa de GPO de la aplicación Citrix Workspace.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Plantillas administrativas clásicas (ADM)** > **Componentes de Citrix** > **Citrix Workspace** > **StoreFront**.
3. Seleccione **Lista de cuentas de StoreFront/URL de Citrix Gateway**.
4. Seleccione la opción **Habilitado** y haga clic en **Mostrar**. Si habilita esta configuración de directiva, puede introducir una lista de cuentas de StoreFront y una URL de NetScaler Gateway.
5. Introduzca la URL en el campo **Valor**.
6. Especifique la URL del almacén que se utiliza con la aplicación Workspace:

   ```
   STOREx="storename;http[s]://servername.domain/IISLocation/discovery;[On, Off]; [storedescription]"
   ```

   Valores:

   - x: Los enteros del 0 al 9 se utilizan para identificar un almacén.
   - storename: Nombre del almacén. Este valor debe coincidir con el nombre configurado en el servidor de StoreFront.
   - servername.domain: El nombre de dominio completo del servidor que aloja el almacén.
   - IISLocation: La ruta al almacén en IIS. La URL del almacén debe coincidir con la URL en el archivo de aprovisionamiento de StoreFront. La URL del almacén tiene el formato "/Citrix/-Store/discovery". Para obtener la dirección URL, exporte un archivo de aprovisionamiento desde StoreFront, ábralo en el Bloc de notas y copie la dirección URL desde el elemento Address.
   -
   - storedescription: Una descripción del almacén, como "Tienda de aplicaciones de RR. HH."
7. Agregue o especifique la URL de Citrix Gateway. Introduzca el nombre de la dirección URL separada por punto y coma:

   Ejemplo: `STORE0= HRStore;https://ag.mycompany.com##Storename;On;Store`
   Donde #Storename es el nombre del almacén detrás de Citrix Gateway.

> **Nota:**
>
> - La URL del almacén de Citrix Gateway debe ser la primera de la lista (parámetro STORE0).
> - En una configuración con varios almacenes, solo se permite la configuración de una URL de almacén de Citrix Gateway.
> - La URL de almacén de Citrix Gateway configurada con este método no admite los sitios de servicios de PNA que utilicen Citrix Gateway.

> - El parámetro `/Discovery` no es necesario cuando se especifica una URL de almacén de Citrix Gateway.

A partir de la versión 1808, los cambios realizados en la directiva URL de Citrix Gateway/Lista de cuentas de StoreFront se aplican en una sesión después de reiniciar la aplicación. No es necesario reiniciarla.

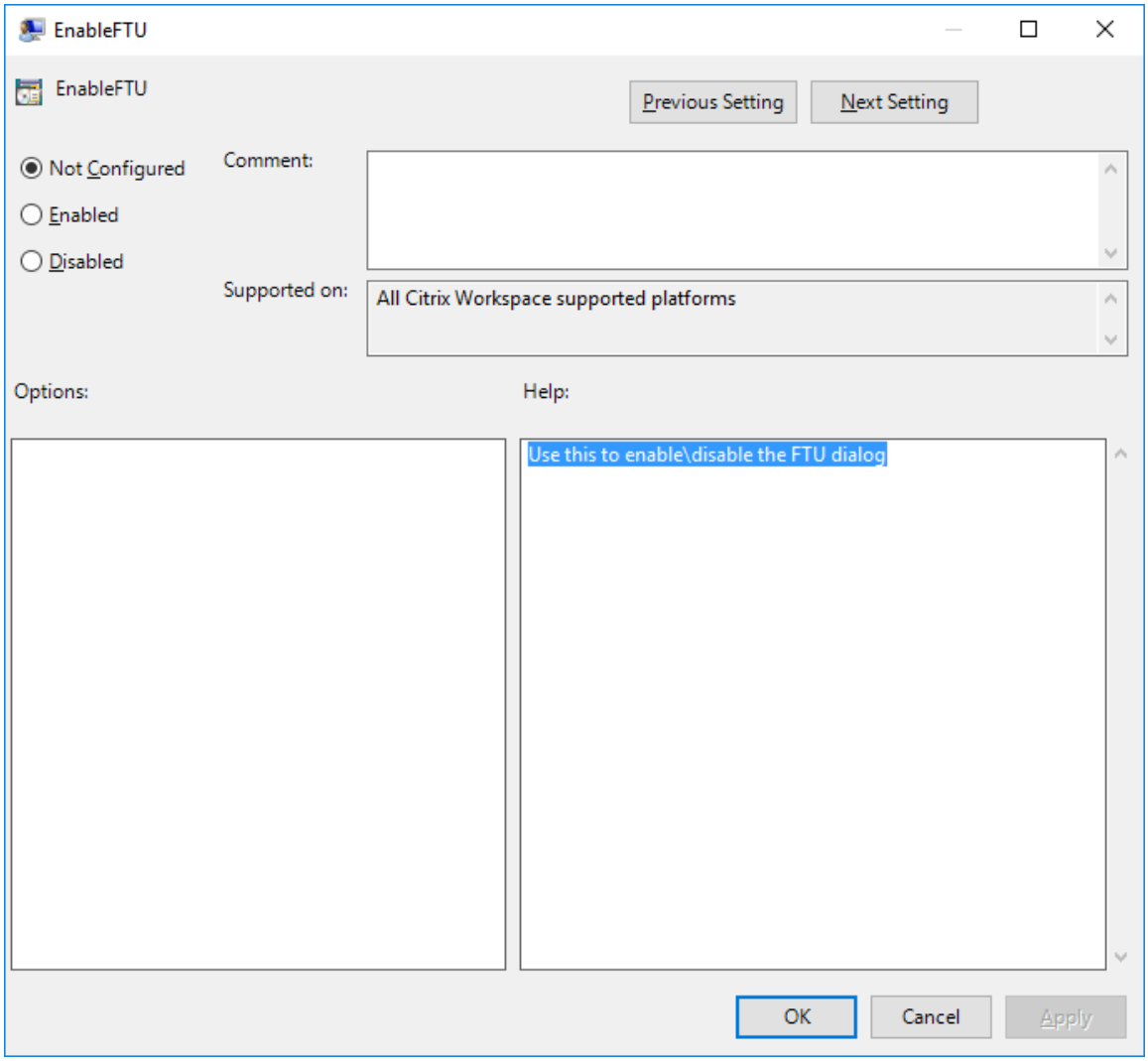
> **Nota:**
>
> En una instalación nueva, no es necesario restablecer la aplicación Citrix Workspace 1808 ni versiones posteriores. Si hay una actualización a 1808 o una versión posterior, debe restablecer la aplicación Citrix Workspace para que los cambios surtan efecto.

**Limitaciones:**

- La URL de Citrix Gateway debe incluirse en primer lugar, seguida de direcciones URL de StoreFront.
- No está disponible la opción de usar varias direcciones URL de Citrix Gateway.

> **Nota:**
>
> Los usuarios también pueden acceder al almacén desde un explorador web. Los usuarios pueden iniciar sesión en Citrix Store desde un explorador web e iniciar una aplicación virtual o un escritorio desde la Web. El inicio de aplicaciones o escritorios virtuales aprovecha las capacidades de la aplicación Citrix Workspace instalada de forma nativa.
>
> En este caso, puede ser conveniente ocultar la solicitud **Agregar cuenta** a los usuarios. Esto se puede hacer mediante la siguiente configuración:
>
> - **Cambiar el nombre del archivo de ejecución de Citrix**: Cambie el nombre de **CitrixWorkspaceApp.exe** a **CitrixWorkspaceAppWeb.exe** para modificar el comportamiento del cuadro de diálogo **Agregar cuenta**. Al cambiar el nombre del archivo, el diálogo **Agregar cuenta** no aparece en el menú **Inicio**.
> - **Plantilla administrativa de GPO**: Para ocultar la opción **Agregar cuenta** en el asistente de instalación de la aplicación Citrix Workspace, inhabilite **EnableFTUpolicy** en el nodo Autoservicio de la plantilla administrativa de GPO, como se muestra a continuación. Como este es un parámetro por máquina, el comportamiento se aplica a todos los usuarios.




### Resolución de nombres de DNS

Puede configurar la aplicación Citrix Workspace para Windows de modo que use Citrix XML Service para solicitar un nombre DNS de un servidor en lugar de una dirección IP.

> **Importante:**
>
> A menos que el entorno DNS esté configurado específicamente para utilizar esta función, Citrix recomienda no habilitar la resolución de nombres DNS en el servidor.

De forma predeterminada, la resolución de nombres DNS está inhabilitada en el servidor y habilitada en la aplicación Citrix Workspace. Cuando la resolución de nombres DNS está inhabilitada en el servidor, todas las solicitudes de la aplicación Citrix Workspace de un nombre DNS devuelven una dirección IP. No es necesario inhabilitar la resolución de nombres DNS en la aplicación Citrix Workspace.

Para inhabilitar la resolución de nombres DNS para dispositivos cliente específicos:

Si su implementación de servidores usa DNS para la resolución de nombres y tiene problemas con algunos dispositivos de usuario, puede inhabilitar la resolución de nombres DNS para esos dispositivos.

> **Precaución:**
>
> Es posible que el uso incorrecto del Editor del Registro del sistema cause problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

1. Agregue una cadena de clave de Registro **xmlAddressResolutionType** a `HKEY\\_LOCAL\\_MACHINE\Software\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing`.
2. El valor debe ser **IPv4-Port**.
3. Repita el proceso para cada usuario de los dispositivos de usuario.

## Conectar

La aplicación Citrix Workspace ofrece a los usuarios acceso de autoservicio seguro a aplicaciones y escritorios virtuales, y acceso a demanda a aplicaciones de Windows, web y de Software como servicio (SaaS). Las páginas web de Citrix StoreFront, o las páginas web antiguas creadas con la Interfaz Web, administran el acceso de los usuarios.

### Para conectarse a los recursos mediante la interfaz de usuario de Citrix Workspace

La página de inicio de la aplicación Citrix Workspace muestra las aplicaciones y los escritorios virtuales que están disponibles para los usuarios, basándose en los parámetros de cuenta del usuario (es decir, el servidor al que se conecta) y en los parámetros configurados por los administradores de Citrix Virtual Apps and Desktops o Citrix DaaS. Desde la página **Preferencias** > **Cuentas**, puede configurar la dirección URL de un servidor de StoreFront o, si está configurada la detección de cuentas basada en correo electrónico, escribir la dirección de correo electrónico.

Después de conectarse a un almacén, el autoservicio muestra las fichas **Favoritos**, **Escritorios** y **Aplicaciones**. Para iniciar una sesión, haga clic en el icono correspondiente. Para agregar un icono a **Favoritos**, haga clic en el icono **...** y seleccione **Agregar a Favoritos**.

# Configurar

April 6, 2023

Al utilizarse la aplicación Citrix Workspace para Windows, los parámetros siguientes permiten a los usuarios acceder a sus aplicaciones y escritorios alojados.

## Tareas y aspectos relevantes para administradores

En este artículo se describen las tareas y los aspectos que son relevantes para los administradores de la aplicación Citrix Workspace para Windows.

### Administrar marcas de función

Si se produce un problema con la aplicación Citrix Workspace en producción, podemos inhabilitar de manera dinámica una función afectada en la aplicación Citrix Workspace aunque dicha función ya se haya publicado.

Para ello, se utilizan marcas de función y un servicio externo denominado LaunchDarkly. No es necesario que realice ninguna configuración para permitir el tráfico a LaunchDarkly, salvo si tiene un firewall o proxy bloqueando el tráfico saliente. En ese caso, puede habilitar el tráfico a LaunchDarkly a través de direcciones URL o direcciones IP específicas, según sus requisitos de directiva.

Puede habilitar el tráfico y la comunicación en LaunchDarkly de las siguientes formas:

### Permitir el tráfico a las siguientes URL

- `events.launchdarkly.com`
- `stream.launchdarkly.com`
- `clientstream.launchdarkly.com`
- `Firehose.launchdarkly.com`
- `mobile.launchdarkly.com`

### Incluir direcciones IP en una lista de permitidos

Si necesita incluir las direcciones IP en una lista de permitidos, para obtener una lista de todos los intervalos de direcciones IP actuales, consulte esta lista de direcciones IP públicas de LaunchDarkly. Puede usar esta lista para saber que las configuraciones de su firewall se actualizan automáticamente de acuerdo con las actualizaciones de la infraestructura. Para obtener detalles sobre el estado actual de los cambios en la infraestructura, consulte la Página de estado de LaunchDarkly.

#### Requisitos del sistema para LaunchDarkly

Compruebe si las aplicaciones pueden comunicarse con los siguientes servicios si el parámetro de túnel dividido está **desactivado** en Citrix ADC para estos servicios:

- Servicio de LaunchDarkly.
- Servicio de escucha de APNs

#### Inhabilitar el servicio de LaunchDarkly

Puede inhabilitar el servicio de LaunchDarkly mediante una directiva de objeto de directiva de grupo (GPO).

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Conformidad**.
3. Seleccione **Inhabilitar el envío de datos a terceros** y actívelo.
4. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**

### Plantilla administrativa de objetos de directiva de grupo

Se recomienda utilizar la plantilla administrativa de objetos de directiva de grupo y configurar reglas para:

- Redirección de red
- Servidores proxy
- Configuración del servidor de confianza
- Redirección de usuarios
- Dispositivos de usuarios remotos
- Experiencia del usuario.

Puede utilizar los archivos de plantilla `receiver.admx` o `receiver.adml` con directivas de dominio y de equipos locales. Para las directivas de dominio, importe el archivo de plantilla mediante la Consola de administración de directivas de grupo. La importación es útil al aplicar los parámetros de la aplicación Citrix Workspace a diferentes dispositivos de usuario en la empresa. Para modificar un solo dispositivo de usuario, importe el archivo de plantilla mediante el Editor de directivas de grupo local del dispositivo.

Citrix recomienda utilizar la plantilla administrativa de GPO de Windows para configurar la aplicación Citrix Workspace.

El directorio de instalación incluye `CitrixBase.admx` y `CitrixBase.adml`, así como los archivos de plantillas administrativas (`receiver.adml` o `receiver.admx`‘receiver.adml‘).

> **Nota:**
>
> Los archivos ADMX y ADML se utilizan con la versión de Windows mencionada en la Tabla de compatibilidad.

Si la aplicación Citrix Workspace se instala con el VDA, los archivos ADMX/ADML suelen encontrarse en el directorio `\<installation directory>\Online Plugin\Configuration`.

Si la aplicación Citrix Workspace se instala sin el VDA, los archivos ADMX/ADML suelen encontrarse en el directorio `C:\Program Files\Citrix\ICA Client\Configuration`.

Consulte la tabla siguiente para obtener información sobre los archivos de plantilla de aplicaciones de Citrix Workspace y sus respectivas ubicaciones.

> **Nota:**
>
> Citrix recomienda usar los archivos de plantilla de objetos de directiva de grupo (GPO) proporcionados con la versión más reciente de la aplicación Citrix Workspace.

| Tipo de archivo | Ubicación de archivos |
|---|---|
| receiver.adm | \<Directorio de instalación\>\\ICA Client\\Configuration |
| receiver.admx | \<Directorio de instalación\>\\ICA Client\\Configuration |
| receiver.adml | \<Directorio de instalación\>\\ICA Client\\Configuration\\\[MUIculture\] |
| CitrixBase.admx | \<Directorio de instalación\>\\ICA Client\\Configuration |
| CitrixBase.adml | \<Directorio de instalación\>\\ICA Client\\Configuration\\\[MUIculture\] |

> **Nota:**
>
> - Si no se agrega CitrixBase.admx\adml al GPO local, se puede perder la directiva **Habilitar ICA File Signing**.
> - Al actualizar la versión de la aplicación Citrix Workspace, agregue los archivos de plantilla más recientes al GPO local. La configuración anterior se conserva después de la importación. Para obtener más información, consulte el siguiente procedimiento:

**Para agregar los archivos de plantilla receiver.admx/adml al objeto de directiva de grupo local:**

Puede utilizar archivos de plantilla ADM para configurar los objetos de directiva de grupo locales y aquellos que utilizan dominios. Consulte aquí el artículo de Microsoft MSDN acerca de la adminis-

tración de archivos ADMX.

Después de instalar la aplicación Citrix Workspace, copie estos archivos de plantilla:

| Tipo de archivo | Copiar de | Copiar a |
|---|---|---|
| receiver.admx | `Installation Directory\ICA Client\Configuration\receiver.admx` | `%systemroot%\policyDefinitions` |
| CitrixBase.admx | `Installation Directory\ICA Client\Configuration\CitrixBase.admx` | `%systemroot%\policyDefinitions` |
| receiver.adml | `Installation Directory\ICA Client\Configuration\[MUIculture]receiver.adml` | `%systemroot%\policyDefinitions\[MUIculture]` |
| CitrixBase.adml | `Installation Directory\ICA Client\Configuration\[MUIculture]\CitrixBase.adml` | `%systemroot%\policyDefinitions\[MUIculture]` |

> **Nota:**
>
> Agregue CitrixBase.admx/CitrixBase.adml a la carpeta `\PolicyDefinitions` para ver los archivos de plantilla en **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace**.

## Protección de aplicaciones

> **Renuncia de responsabilidades**
>
> Las directivas de protección de aplicaciones filtran el acceso a las funciones requeridas del sistema operativo subyacente (llamadas a API específicas necesarias para capturar pantallas o pulsaciones de teclas). Las directivas de protección de aplicaciones proporcionan protección incluso contra herramientas de piratas informáticos personalizadas y con un diseño específico. Sin embargo, a medida que los sistemas operativos evolucionan, es posible que surjan nuevas for-

> mas de capturar pantallas y registrar pulsaciones de teclas. Si bien seguimos identificándolas y abordándolas, no podemos garantizar una protección completa en configuraciones e implementaciones específicas.

Protección de aplicaciones es una función complementaria que proporciona una mayor seguridad al usar Citrix Virtual Apps and Desktops y Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service). La función restringe la posibilidad de que los clientes puedan verse amenazados por malware de registro de pulsaciones de teclas y malware de capturas de pantalla. La protección de aplicaciones evita la exfiltración de información confidencial, como credenciales de usuario e información confidencial en pantalla. La función evita que los usuarios y los atacantes hagan capturas de pantalla y usen registradores de pulsaciones de teclas para obtener y explotar información confidencial.

La protección de aplicaciones requiere instalar una licencia adicional en el servidor de licencias. También debe haber presente una licencia de Citrix Virtual Desktops. Para obtener información sobre las licencias, consulte la sección Configuración de la documentación de Citrix Virtual Apps and Desktops.

**Requisitos:**

- Citrix Virtual Apps and Desktops 1912 o versiones posteriores.
- StoreFront versión 1912 o Workspace.
- Aplicación Citrix Workspace 1912 o versiones posteriores.

**Requisitos previos:**

- La función de protección de aplicaciones debe estar habilitada en el Controller. Para obtener más información, consulte la sección Protección de aplicaciones en la documentación de Citrix Virtual Apps and Desktops.

> **Nota:**
>
> - Esta función solo está disponible en sistemas operativos de escritorio como Windows 11, Windows 10 o Windows 8.1.
> - A partir de la versión 2006.1, la aplicación Citrix Workspace no se admite en Windows 7. Por lo tanto, la protección de aplicaciones no funciona en Windows 7. Para obtener más información, consulte Elementos retirados.
> - Esta función no se puede usar con el Protocolo de escritorio remoto (RDP).

**Protección de sesiones HDX locales:**

Dos directivas proporcionan funciones contra el registro de tecleo y las capturas de pantalla en las sesiones. Estas directivas deben configurarse a través de PowerShell. No hay ninguna GUI disponible para este propósito.

> **Nota:**
>
> A partir de la versión 2103, Citrix DaaS ofrece la protección de aplicaciones con StoreFront y

> Workspace.

Para obtener información sobre la configuración de la protección de aplicaciones en Citrix Virtual Apps and Desktops y Citrix DaaS, consulte Protección de aplicaciones.

**Protección de aplicaciones: Configuración en la aplicación Citrix Workspace**

El componente Protección de aplicaciones ahora se instala de forma predeterminada durante la instalación de la aplicación Citrix Workspace.

La casilla **Habilitar protección de aplicaciones** que aparece durante la instalación se sustituye por **Iniciar protección de aplicaciones tras la instalación**.


Al seleccionar esta casilla de verificación, Protección de aplicaciones se inicia inmediatamente después de la instalación.

> **Nota:**
>
> Si no se habilita esta casilla de verificación, Protección de aplicaciones se inicia automáticamente al iniciar por primera vez un recurso o componente protegido en el caso de los clientes que tienen asignado el derecho de uso del componente Protección de aplicaciones.

**Interfaz de la línea de comandos**

También puede iniciar el componente Protección de aplicaciones mediante el parámetro /`startappprotection` de línea de comandos. Sin embargo, el conmutador /`includeappprotection` anterior se ha retirado.

La tabla siguiente proporciona información sobre las pantallas protegidas en función de la implementación:

| Implementación de la protección de aplicaciones | Pantallas protegidas | Pantallas no protegidas |
|---|---|---|
| Se incluye en la aplicación Citrix Workspace | Cuadro de diálogo de credenciales de usuario / administrador de autenticación y Self-Service Plug-in | Central de conexiones, Dispositivos, cualquier mensaje de error de la aplicación Citrix Workspace, Reconexión automática de clientes, Agregar cuenta |
| Se ha configurado en el Controller | Pantalla de sesión ICA (tanto aplicaciones como escritorios) | Central de conexiones, Dispositivos, cualquier mensaje de error de la aplicación Citrix Workspace, Reconexión automática de clientes, Agregar cuenta |

Al tomar una captura de pantalla, solo se oscurece la ventana protegida. Puede hacer una captura de pantalla de la zona que queda fuera de la ventana protegida. Sin embargo, si utiliza la tecla Impr Pant para hacer una captura de pantalla en un dispositivo con Windows 10, debe minimizar la ventana protegida.

Anteriormente, las funcionalidades de protección contra la captura de tecleo y contra las capturas de pantalla se aplicaban de forma predeterminada para la autenticación de Citrix y las pantallas de la aplicación Citrix Workspace. Sin embargo, a partir de 2212, estas capacidades están inhabilitadas de forma predeterminada y deben configurarse mediante el objeto de directiva de grupo.

> **Nota:**
>
> Esta directiva de GPO no se aplica a las sesiones ICA y SaaS. Las sesiones ICA y SaaS se siguen controlando mediante el Delivery Controller y Citrix Secure Private Access.

**Configurar la protección de aplicaciones para la interfaz del Self-Service Plug-in**

1. Ejecute `gpedit.msc` para abrir la plantilla administrativa de GPO de la aplicación Citrix Workspace.

2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace**.
3. Para configurar la protección contra el registro de tecleo y la protección contra capturas de pantalla para el cuadro de diálogo del Self-Service Plug-in, seleccione **Autoservicio** > directiva **Administrar protección de aplicaciones**.
4. Seleccione una de estas opciones o las dos:
   - **Protección contra el registro de tecleo**: Evita que programas capturen tecleo.
   - **Protección contra capturas de pantalla**: Evita que los usuarios realicen capturas de pantalla y compartan su pantalla.
5. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**

**Configurar la protección de aplicaciones para el administrador de autenticación**

1. Ejecute `gpedit.msc` para abrir la plantilla administrativa de GPO de la aplicación Citrix Workspace.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace**.
3. Para configurar la protección contra el registro de tecleo y la protección contra capturas de pantalla para el administrador de autenticación, seleccione **Autenticación de usuarios** > directiva **Administrar protección de aplicaciones**.
4. Seleccione una de estas opciones o las dos:
   - **Protección contra el registro de tecleo**: Evita que programas capturen tecleo.
   - **Protección contra capturas de pantalla**: Evita que los usuarios realicen capturas de pantalla y compartan su pantalla.
5. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**

**Comportamiento previsto:**

El comportamiento previsto depende del método por el cual los usuarios acceden al almacén de StoreFront que tiene los recursos protegidos.

> **Nota:**
>
> - Citrix recomienda que utilice la aplicación Citrix Workspace nativa únicamente para iniciar sesiones protegidas.

## Mejora de la protección de aplicaciones: Detección y notificación de capturas de pantalla

A partir de la versión 2212 de la aplicación Citrix Workspace para Windows, podrá ver una notificación cuando haya un posible intento de captura de pantalla con relación a cualquier recurso protegido.

Para obtener información sobre los recursos protegidos con Protección de aplicaciones, consulte ¿Qué protege la protección de aplicaciones?

La notificación aparece cuando hay:

- Un intento de hacer una captura de pantalla o grabar un vídeo a través de una herramienta para captura de pantallas.
- Un intento de hacer una captura de pantalla con la tecla Imprimir pantalla.

> **Nota:**
>
> La notificación aparece solo una vez por instancia en ejecución de la herramienta de captura de pantallas. La notificación vuelve a aparecer si reinicia la herramienta e intenta capturar una pantalla.

## Mejora de la protección de aplicaciones: Configurar la protección de aplicaciones para la autenticación y Self-Service Plug-in mediante Global App Configuration Service

A partir de la versión 2302, la aplicación Citrix Workspace para Windows permite configurar la protección de aplicaciones para la autenticación y Self-Service Plug-in mediante Global App Configuration Service. Anteriormente, solo se podían configurar estos componentes mediante el objeto de directiva de grupo.

Si habilita las funciones de protección contra registro de tecleo y contra la captura de pantalla mediante Global App Configuration Service, se aplicarán tanto a la autenticación como a Self-service Plug-in.

> **Nota:**
>
> Las configuraciones de Global App Configuration Service no afectan a las aplicaciones virtuales, los escritorios virtuales, las aplicaciones web y las aplicaciones SaaS. Estos recursos se siguen controlando mediante el Delivery Controller y Citrix Secure Private Access. Para obtener más información, consulte la sección de configuración de Protección de aplicaciones en la documentación de Citrix Virtual Apps and Desktops.

### Configuración de la protección de aplicaciones para la autenticación y Self-service Plug-in mediante la API del Global App Configuration Service

Los administradores pueden usar la API para configurar estas funciones de la protección de aplicaciones. Los parámetros son los siguientes:

- **Configuración para habilitar o inhabilitar la protección contra capturas de pantalla:**

  “nombre”: “enable anti screen capture for auth and ssp”
  “valor”: “true” o “false”

- **Configuración para habilitar o inhabilitar la protección contra el registro de tecleo:**

  “nombre”: “enable anti key-logging for auth and ssp”
  “valor”: “true” o “false”

Para la configuración, a continuación se muestra un archivo JSON de ejemplo para habilitar las funciones de protección contra capturas de pantalla y contra el registro de tecleo de la aplicación Citrix Workspace para Windows en Global App Configuration Service:

```
{


          "category": "App Protection",

          "userOverride": true,

          "assignedTo": [

            "AllUsersNoAuthentication"

          ],

          "settings": [

            {


              "name": "enable anti screen capture for auth and ssp",

              "value": true

             }
 ,

            {


              "name": "enable anti key-logging for auth and ssp",

              "value": true

             }


          ] }
```

### Nota adicional

- **Comportamiento en los espacios de trabajo para la web:**

  El componente de protección de aplicaciones no se admite en las configuraciones de espacios de trabajo para la web. Las aplicaciones protegidas por directivas de protección de aplicaciones no se indican. Para obtener más información acerca de los recursos asignados, póngase en contacto con el administrador del sistema.

- **Comportamiento de las versiones de la aplicación Citrix Workspace que no ofrecen la protección de aplicaciones:**

  En la versión 1911 de la aplicación Citrix Workspace y en versiones anteriores, las aplicaciones protegidas por directivas de protección de aplicaciones no se indican en StoreFront.

- **Comportamiento de las aplicaciones que tienen configurada la función de protección de aplicaciones en el Controller:**

  En un Controller configurado con protección de aplicaciones, si intenta iniciar una aplicación protegida, la protección de aplicaciones se inicia automáticamente y protege la aplicación.

- **Comportamiento de la sesión protegida en caso de protocolo de escritorio remoto (RDP)**
  - La sesión protegida activa se desconecta si se inicia una sesión de protocolo RDP.
  - No puede iniciar sesiones protegidas en sesiones con Protocolo de escritorio remoto (RDP).

#### Registros de errores de la protección de aplicaciones

A partir de la versión 2103, los registros de protección de aplicaciones se recopilan como parte de los registros de la aplicación Citrix Workspace. Para obtener más información sobre la recopilación de registros, consulte Recopilación de registros.

#### Desinstalar el componente de protección de aplicaciones

Para desinstalar el componente de protección de aplicaciones, debe desinstalar la aplicación Citrix Workspace del sistema. Reinicie el sistema para que los cambios surtan efecto.

> **Nota:**
>
> La protección de aplicaciones solo se ofrece en la actualización que hay a partir de la versión 1912.

#### Problemas conocidos y limitaciones

- Una vez que se haya iniciado un escritorio protegido, también se protegerán las sesiones de escritorio que ya estén activas y las que se inicien posteriormente. Esta es una limitación cono-

cida, ya que el proceso del lado del cliente denominado `CDViewer.exe` es el mismo para todas las sesiones de escritorio. Sin embargo, esta limitación no debería estar en sesiones de aplicaciones.
- Esta función no está disponible en sistemas operativos de Microsoft Server, como Windows Server 2012 R2 y Windows Server 2016.
- Esta función no está disponible en casos de doble salto.
- Para que esta función opere correctamente, inhabilite la directiva **Redirección del portapapeles del cliente** del VDA.

### Categorías de las aplicaciones

Las categorías de las aplicaciones permiten a los usuarios administrar colecciones de aplicaciones en la aplicación Citrix Workspace. Puede crear grupos de aplicaciones para aplicaciones compartidas en diferentes grupos de entrega o utilizadas por un subconjunto de usuarios dentro de los grupos de entrega.

Para obtener más información, consulte Crear grupos de aplicaciones en la documentación de Citrix Virtual Apps and Desktops.

### Seguridad de archivos ICA mejorada

Esta función proporciona una mayor seguridad al gestionar archivos ICA durante el inicio de sesiones de aplicaciones y escritorios virtuales.

Ahora, la aplicación Citrix Workspace le permite almacenar el archivo ICA en la memoria del sistema en lugar de hacerlo en el disco local al iniciar sesiones de aplicaciones y escritorios virtuales.

Esta función tiene como objetivo eliminar los ataques de superficie y cualquier malware que pueda utilizar incorrectamente el archivo ICA al almacenarlo localmente. Esta función también se puede aplicar a las sesiones de aplicaciones y escritorios virtuales que se inician en Workspace para Web

#### Configuración

La seguridad de archivos ICA también se ofrece al acceder a Citrix Workspace o a StoreFront desde la web. La detección de clientes es un requisito previo para que la función esté operativa si se accede a través de la web. Si accede a StoreFront mediante un explorador, habilite estos atributos en el archivo web.config de las implementaciones de StoreFront:

| Versión de StoreFront | Atributo |
|---|---|
| 2.x | pluginassistant |
| 3.x | protocolHandler |

Cuando inicie sesión en el almacén a través del explorador web, haga clic en **Detectar la aplicación Workspace**. Si no aparece la solicitud, borre las cookies del explorador web e inténtelo de nuevo.

Si se trata de una implementación de Workspace, los parámetros de detección de clientes se encuentran en **Parámetros de cuenta** > **Avanzado** > **Preferencia de inicio de aplicaciones y escritorios**.

Puede tomar medidas adicionales para que las sesiones se inicien solo con el archivo ICA almacenado en la memoria del sistema. Utilice cualquiera de estos métodos:

- Plantilla administrativa de objetos de directiva de grupo (GPO) en el cliente.
- Global App Config Service
- Workspace para Web.

**Mediante el GPO:**

Para bloquear los inicios de sesión desde archivos ICA almacenados en el disco local, haga lo siguiente:

1. Ejecute `gpedit.msc` para abrir la plantilla administrativa de GPO de la aplicación Citrix Workspace.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Motor de cliente**.
3. Seleccione la directiva **Proteger inicio de sesiones con archivos ICA** y **habilítela**.
4. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**

**Mediante Global App Config Service:**

Puede usar Global App Config Service desde la aplicación Citrix Workspace 2106.

Para bloquear los inicios de sesión desde archivos ICA almacenados en el disco local, haga lo siguiente:

Establezca el atributo **Bloquear el inicio directo del archivo ICA** en **True**.

Para obtener más información sobre Global App Config Service, consulte la documentación de Global App Config Service.

**Con Workspace para Web:**

Para no permitir la descarga de archivos ICA en el disco local al usar Workspace para Web, haga lo siguiente:

Ejecute el módulo de PowerShell. Consulte Configure DisallowICADownload.

> **Nota:**
>
> La directiva **DisallowICADownload** no está disponible para implementaciones de StoreFront.

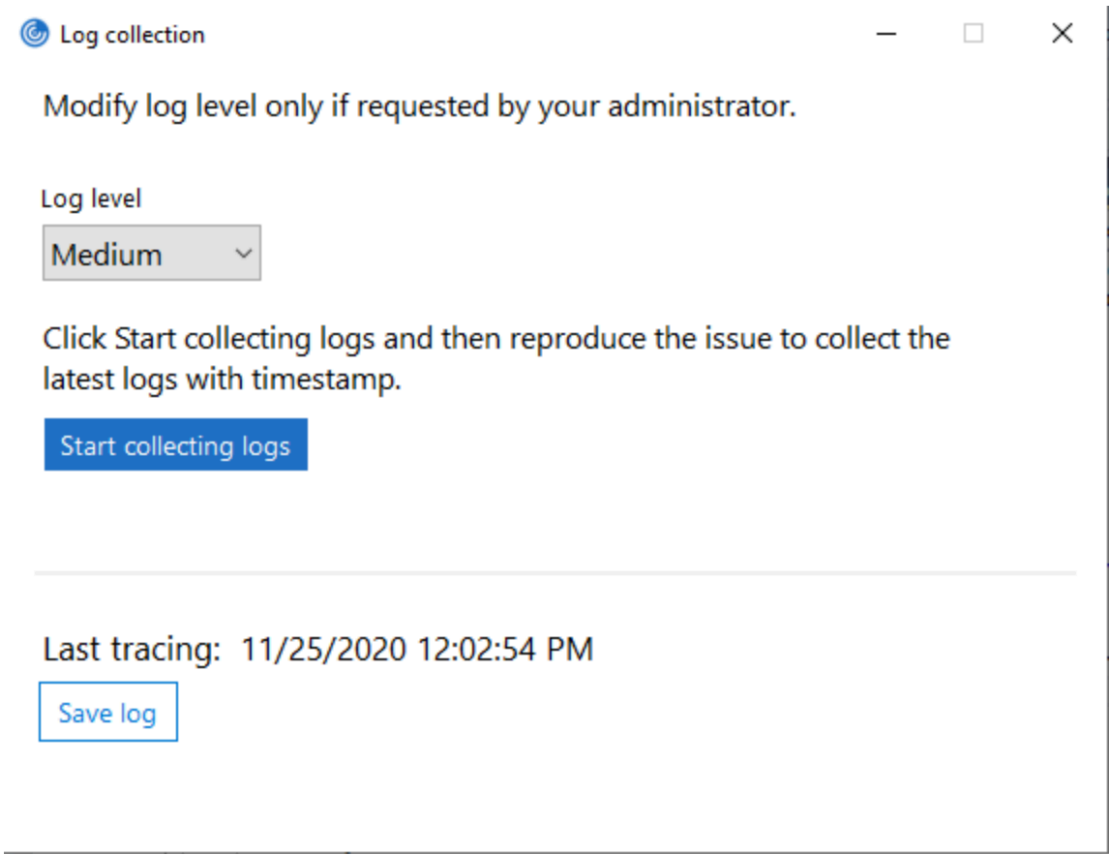
### Recopilación de registros

La recopilación de registros simplifica el proceso de recopilación de registros para la aplicación Citrix Workspace. Los registros ayudan a Citrix a solucionar problemas y, en el caso de problemas complicados, facilitan la asistencia técnica.

Puede recopilar registros mediante la interfaz gráfica de usuario.

**Recopilación de registros:**

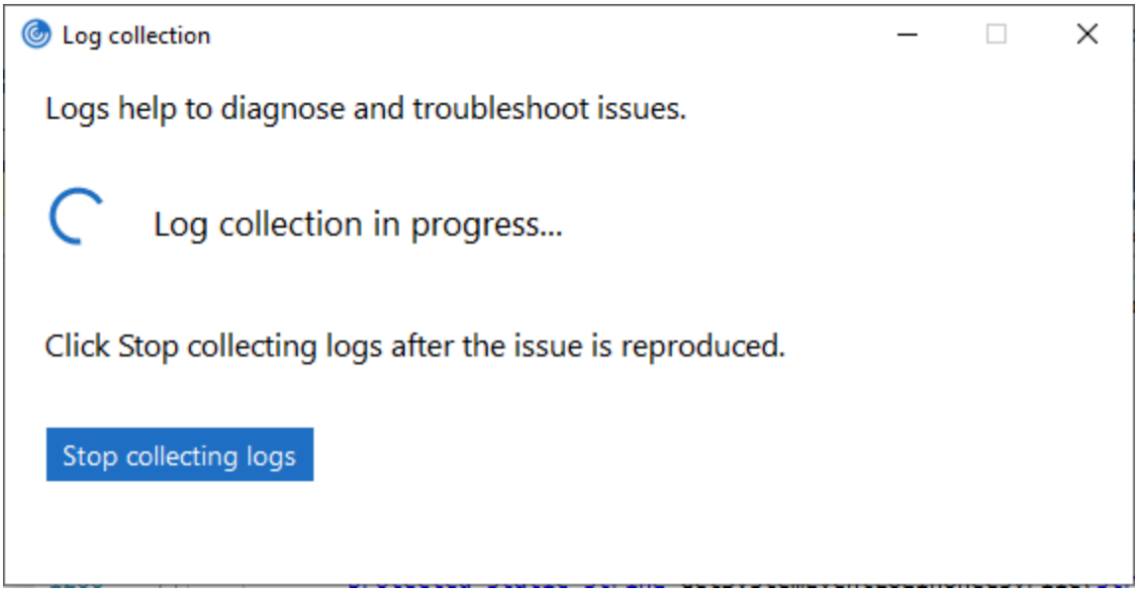
1. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace en el área de notificaciones y seleccione **Preferencias avanzadas**.
2. Seleccione **Recopilación de registros**.
   Aparecerá el cuadro de diálogo Recopilación de registros.




3. Seleccione uno de los siguientes niveles de registros:
   - Bajo
   - Medio
   - Detallado
4. Haga clic en **Comenzar a recopilar registros** para reproducir el problema y recopilar los registros más recientes.

Se inicia el proceso de recopilación de registros.




5. Haga clic en **Dejar de recopilar registros** una vez reproducido el problema.
6. Haga clic en **Guardar registro** para guardar los registros en la ubicación deseada.

### Rendimiento HDX adaptable

El rendimiento HDX adaptable ajusta de manera inteligente el rendimiento máximo de la sesión ICA porque adapta los búferes de salida. Al principio, la cantidad de búferes de salida se establece en un valor alto. Este valor alto permite que los datos se transmitan al cliente de manera más rápida y eficiente, especialmente en redes de latencia alta.

Así, se obtiene una mejor interactividad, transferencias de archivos más rápidas, reproducciones de vídeo más fluidas, mayor velocidad de fotogramas y mayor resolución en una experiencia de usuario mejorada.

La interactividad de la sesión se mide constantemente para determinar si algún flujo de datos de la sesión ICA está afectando negativamente a la interactividad. Si eso ocurre, el rendimiento se reduce para disminuir el impacto del flujo de datos de gran tamaño en la sesión y permitir que se recupere la interactividad.

Esta función solo se admite en la aplicación Citrix Workspace 1811 para Windows y versiones posteriores.

> **Importante:**
>
> El rendimiento HDX adaptable cambia los búferes de salida al transferir el mecanismo del cliente al VDA. Por lo tanto, adaptar la cantidad de búferes de salida presentes en el cliente como se

> describe en el artículo CTX125027 no produce ningún efecto.

### Transporte adaptable

El transporte adaptable es un mecanismo de Citrix Virtual Apps and Desktops y Citrix DaaS que permite utilizar Enlightened Data Transport (EDT) como protocolo de transporte para conexiones ICA. Para obtener más información, consulte la sección Transporte adaptable en la documentación de Citrix Virtual Apps and Desktops.

### Hoja de Preferencias avanzadas

Puede personalizar la disponibilidad de la hoja **Preferencias avanzadas** y el contenido que figura en el menú contextual del icono de la aplicación Citrix Workspace del área de notificaciones. Al hacerlo, garantiza que los usuarios puedan aplicar solo los parámetros especificados por el administrador en sus sistemas. Específicamente, puede:

- Ocultar la hoja entera de Preferencias avanzadas
- Ocultar los parámetros siguientes:
  - Recopilación de datos
  - Central de conexiones
  - Configuration Checker
  - Barra de idioma y teclado
  - PPP elevados
  - Información de asistencia
  - Accesos directos y reconexión
  - Citrix Files
  - Citrix Casting

#### Ocultar la opción Preferencias avanzadas en el menú contextual

Puede ocultar la hoja “Preferencias avanzadas” mediante la plantilla administrativa de objetos de directiva de grupo (GPO) de la aplicación Citrix Workspace:

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Citrix Workspace** > **Autoservicio** > **Opciones de Preferencias avanzadas**.
3. Seleccione la directiva **Inhabilitar Preferencias avanzadas**.
4. Seleccione **Habilitada** para ocultar la opción “Preferencias avanzadas” en el menú contextual del icono de la aplicación Citrix Workspace en el área de notificaciones.

> **Nota:**
>
> De forma predeterminada, está seleccionada la opción **No configurada**.

**Ocultar parámetros concretos de la hoja de Preferencias avanzadas**

Puede ocultar parámetros específicos configurables por el usuario en la hoja **Preferencias avanzadas** mediante la plantilla administrativa de GPO de la aplicación Citrix Workspace. Para ocultar los parámetros:

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Citrix Workspace** > **Autoservicio** > **Opciones de Preferencias avanzadas**.
3. Seleccione la directiva para el parámetro que quiere ocultar.

Esta tabla contiene las opciones que puede seleccionar y el efecto de cada una:

| Opciones | Acción |
|---|---|
| No configurado | Muestra el parámetro |
| Habilitado | Oculta el parámetro |
| Inhabilitado | Muestra el parámetro |

Puede ocultar los siguientes parámetros concretos en la hoja de Preferencias avanzadas:

- Configuration Checker
- Central de conexiones
- PPP elevados
- Recopilación de datos
- Eliminar contraseñas guardadas
- Barra de idioma y teclado
- Accesos directos y reconexión
- Información de asistencia
- Citrix Files
- Citrix Casting

#### Ocultar la opción de Restablecer Workspace en la hoja de Preferencias avanzadas mediante el Editor del Registro

Puede ocultar opción **Restablecer Workspace** en la hoja "Preferencias avanzadas" solamente mediante el Editor del Registro.

1. Abra el Editor del Registro.
2. Vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`.
3. Cree una clave de valor de cadena **EnableFactoryReset** y configúrela con cualquiera de las siguientes opciones:
    - True: Muestra la opción "Restablecer Workspace" en la hoja "Preferencias avanzadas"
    - False: Oculta la opción "Restablecer Workspace" en la hoja "Preferencias avanzadas"

#### Ocultar la opción de Actualizaciones de Citrix Workspace en la hoja de Preferencias avanzadas

> **Nota:**
>
> La ruta de la directiva para la opción "Actualizaciones de Citrix Workspace" es diferente de la de otras opciones presentes en la hoja "Preferencias avanzadas".

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Actualizaciones de Citrix Workspace**.
3. Seleccione la directiva **Actualizaciones de Citrix Workspace**.
4. Seleccione **Inhabilitada** para ocultar los parámetros de las actualizaciones de Citrix Workspace en la hoja **Preferencias avanzadas**.

### Migración de URL de StoreFront a Workspace

La migración de URL de StoreFront a Workspace le permite migrar fácilmente a los usuarios finales de un almacén de StoreFront a un almacén de Workspace con una interacción mínima de los usuarios.

Tenga en cuenta que todos los usuarios finales tienen un almacén de StoreFront `storefront.com` agregado a su aplicación Workspace. Como administrador, puede configurar una asignación de URL de StoreFront a una URL del espacio de trabajo {'storefront.com':'xyz.cloud.com'} en Global App Configuration Service. Global App Config Service envía la configuración a todas las instancias de la aplicación Citrix Workspace, tanto a dispositivos administrados como a no administrados, que tienen agregada la URL de StoreFront `storefront.com`.

Tras detectarse este parámetro, la aplicación Citrix Workspace agrega la URL del espacio de trabajo asignada `xyz.cloud.com` como otro almacén. Cuando el usuario final inicia la aplicación Citrix Workspace, se abre el almacén de Citrix Workspace. El almacén de StoreFront `storefront.com` agregado anteriormente se agrega a la aplicación Workspace. Los usuarios siempre pueden volver

al almacén de StoreFront `storefront.com` mediante la opción **Cambiar de cuenta** en la aplicación Workspace. Los administradores pueden controlar la eliminación del almacén de StoreFront `storefront.com` de la aplicación Workspace en los dispositivos de punto final. Se puede eliminar a través de Global App Config Service.

Para habilitar la función, siga estos pasos:

1. Configure esta asignación de StoreFront a Workspace mediante Global App Config Service. Para obtener más información sobre Global App Config Service, consulte Global App Configuration Service.
2. Modifique la carga útil en el servicio de configuración de aplicaciones:

```
{

 "serviceURL": {

"url": "https://storefront.acme.com:443",
"migrationUrl": [
  {

    "url": "https://sampleworkspace.cloud.com:443",
    "storeFrontValidUntil": "2023-05-01"
   }

 ]
 }
 ,
"settings": {

"name": "Productivity Apps",
"description": "Provides access StoreFront to Workspace Migration"
   ,
"useForAppConfig": true,
"appSettings": {

  "windows": [
    {

      "category": "root",
      "userOverride": false,
      "assignmentPriority": 0,
      "assignedTo": [
        "AllUsersNoAuthentication"
     ],
      "settings": [
```

```
33         {
34
35          "name": "Hide advanced preferences",
36           "value": false
37          }
38
39        ]
40        }
41
42      ]
43      }
44
45    }
46
47  }
48
49
50 <!--NeedCopy-->
```

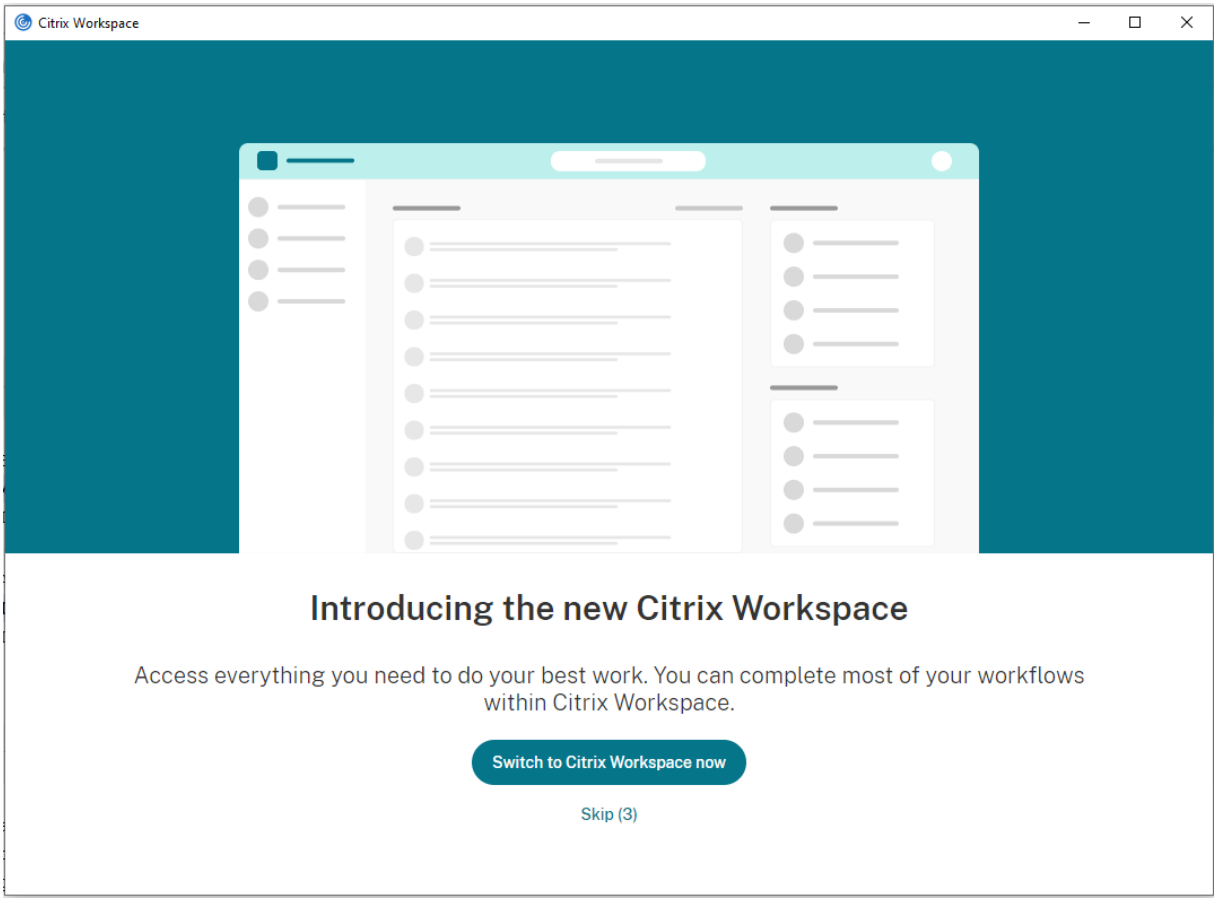
> **Nota:**
>
> Si piensa configurar la carga útil por primera vez, use `POST`.
> Si piensa modificar la configuración de la carga útil existente, utilice `PUT` y compruebe que tiene una carga útil que consta de todos los parámetros compatibles.

3. Especifique la URL de StoreFront `storefront.com` como el valor de **URL** en la sección **serviceURL**.
4. Configure la URL del espacio de trabajo `xyz.cloud.com` en la sección **migrationUrl**.
5. Utilice **storeFrontValidUntil** para establecer el calendario de la eliminación del almacén de StoreFront de la aplicación Workspace. Este campo es opcional. Puede establecer este valor según lo que necesite:
   - Fecha válida en el formato (AAAA-MM-DD)

     > **Nota:**
     >
     > Si proporcionó una fecha anterior, el almacén de StoreFront se quita inmediatamente después de la migración de la URL. Si proporcionó una fecha futura, el almacén de StoreFront se quitará en la fecha establecida.

Una vez enviados los parámetros del servicio de configuración de aplicaciones, aparece esta pantalla:




Cuando el usuario hace clic en **Cambiar a Citrix Workspace**, la URL del espacio de trabajo se agrega a la aplicación Citrix Workspace y aparece la solicitud de autenticación. Los usuarios tienen una opción limitada de retrasar la transición hasta tres veces.

### Entrega de aplicaciones

Cuando entregue aplicaciones con Citrix Virtual Apps and Desktops y Citrix DaaS, tenga en cuenta las siguientes opciones para mejorar la experiencia de los usuarios:

- Modo de acceso web: Sin configuración necesaria, la aplicación Citrix Workspace ofrece acceso web a las aplicaciones y los escritorios. Puede abrir un explorador web para ir a un sitio de Workspace para Web y, así, seleccionar y usar las aplicaciones que quiera. En este modo, no se colocan accesos directos en el escritorio del usuario.
- Modo de autoservicio: Cuando agrega una cuenta de StoreFront a la aplicación Citrix Workspace o configura esta aplicación para que apunte a un sitio web de StoreFront, puede definir un *modo de autoservicio*. El modo de autoservicio le permite suscribirse a aplicaciones desde la interfaz de usuario de la aplicación Citrix Workspace. La experiencia de usuario mejorada es similar al uso de una tienda de aplicaciones móviles. En el modo de autoservicio, se pueden configurar parámetros de palabra clave para aplicaciones aprovisionadas automáticamente, destacadas

y obligatorias.

> **Nota:**
>
> De forma predeterminada, la aplicación Citrix Workspace permite seleccionar las aplicaciones que aparecerán en su menú Inicio.

- Modo de acceso directo solamente: Los administradores pueden configurar la aplicación Citrix Workspace para que coloque automáticamente accesos directos de aplicaciones y escritorios directamente en el menú Inicio o en el escritorio. La ubicación es similar a la de la aplicación Citrix Workspace Enterprise. El nuevo modo de *accesos directos solamente* permite a los usuarios buscar todas sus aplicaciones publicadas dentro del esquema de navegación de Windows estándar al que están acostumbrados.

Para obtener información, consulte la sección Crear grupos de entrega de la documentación de Citrix Virtual Apps and Desktops.

#### Configurar el modo de autoservicio

Con solo agregar una cuenta de StoreFront a la aplicación Citrix Workspace o configurar la aplicación Citrix Workspace para que apunte a un sitio de StoreFront, puede configurar el modo de autoservicio. La configuración permite a los usuarios suscribirse a aplicaciones desde la interfaz de usuario de Citrix Workspace. La experiencia de usuario mejorada es similar al uso de una tienda de aplicaciones móviles.

> **Nota:**
>
> De forma predeterminada, la aplicación Citrix Workspace permite a los usuarios seleccionar las aplicaciones que quieran ver en su menú Inicio.

En el modo de autoservicio, se pueden configurar parámetros de palabra clave para aplicaciones aprovisionadas automáticamente, destacadas y obligatorias.

Agregue palabras clave en las descripciones de las aplicaciones de los grupos de entrega:

- Para hacer obligatoria una aplicación concreta (de forma que no pueda eliminarse de la aplicación Citrix Workspace), agregue la cadena KEYWORDS: Mandatory a la descripción de la aplicación. Los usuarios no tienen la opción Quitar para cancelar la suscripción a las aplicaciones obligatorias.
- Para suscribir automáticamente a todos los usuarios de un almacén a una aplicación, agregue la cadena KEYWORDS: Auto a la descripción. Cuando los usuarios inicien sesión en el almacén, la aplicación se aprovisionará automáticamente sin que los usuarios tengan que suscribirse de forma manual a la aplicación.
- Para anunciar aplicaciones a los usuarios o facilitar la búsqueda de las aplicaciones más utilizadas incorporándolas a la lista Destacados de Citrix Workspace, agregue la cadena KEYWORDS: Featured a la descripción de cada aplicación.

**Personalizar las ubicaciones de los accesos directos de aplicaciones mediante la plantilla de objeto de directiva de grupo**

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Autoservicio**.
3. Seleccione la directiva **Administrar modo Self-Service**.
   a) **Habilítela** para ver la interfaz de usuario que ofrece la directiva de autoservicio.
   b) **Inhabilítela** si quiere suscribirse manualmente a las aplicaciones. Esta opción oculta la interfaz de usuario de autoservicio.
4. Seleccione la directiva **Administrar accesos directos de aplicaciones**.
5. Seleccione las opciones según sea necesario.
6. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**
7. Reinicie la aplicación Citrix Workspace para que los cambios surtan efecto.

**Usar parámetros de cuenta de StoreFront para personalizar las ubicaciones de los accesos directos de aplicaciones**

Puede configurar accesos directos en el menú Inicio y en el escritorio desde el sitio de StoreFront. Se puede agregar esta configuración al archivo web.config en `C:\inetpub\wwwroot\Citrix\Roaming`, en la sección **<annotatedServices>**:

- Para poner los accesos directos en el escritorio, use PutShortcutsOnDesktop. Parámetros: “true” o “false” (predeterminado: false).
- Para poner los accesos directos en el menú Inicio, use PutShortcutsInStartMenu. Parámetros: “true” o “false” (predeterminado: true).
- Para usar la ruta de categoría en el menú Inicio, UseCategoryAsStartMenuPath. Parámetros: “true” o “false” (predeterminado: true).

> **Nota:**
>
> Windows 8, Windows 8.1 y Windows 10 no permiten la creación de carpetas anidadas dentro del menú Inicio. En su lugar, muestra las aplicaciones individualmente o en la carpeta raíz. Las aplicaciones no se encuentran en las subcarpetas de categoría definidas con Citrix Virtual Apps and Desktops y Citrix DaaS.

- Para establecer un único directorio para todos los accesos directos del menú Inicio, use `StartMenuDir`. Parámetro: Valor de cadena, correspondiente al nombre de la carpeta donde se van a incluir los accesos directos.
- Para volver a instalar aplicaciones modificadas, use AutoReinstallModifiedApps. Parámetros: “true” o “false” (predeterminado: true).

- Para mostrar un único directorio para todos los accesos directos en el escritorio, use `DesktopDir`. Parámetro: Valor de cadena, correspondiente al nombre de la carpeta donde se van a incluir los accesos directos.
- Para no crear ninguna entrada en los clientes "Agregar o quitar programas", use `DontCreateAddRemoveEnt` . Parámetros: "true" o "false" (predeterminado: false).
- Para quitar los accesos directos y el icono de Citrix Workspace de una aplicación que estuvo disponible en el almacén, pero ya no lo está, use `SilentlyUninstallRemovedResources`. Parámetros: "true" o "false" (predeterminado: false).

En el archivo web.config, los cambios se deben agregar en la sección **XML** de la cuenta. Para encontrar esta sección, busque la etiqueta de apertura:

```
<account id=... name="Store"
```

La sección termina con la etiqueta </account>.

Antes del final de la sección sobre cuentas, en la primera sección sobre propiedades:

```
<properties> <clear> <properties>
```

Se pueden agregar propiedades a esta sección después de la etiqueta <clear />, una por línea, mediante el nombre y el valor. Por ejemplo:

```
<property name="PutShortcutsOnDesktop"value="True"/>
```

> **Nota:**
>
> Es posible que los elementos de propiedad agregados antes de la etiqueta <clear /> los invaliden. Si quiere, puede optar por quitar la etiqueta <clear /> al agregar un nombre y un valor de propiedad.

El siguiente es un ejemplo ampliado para esta sección:

```
<properties <property name="PutShortcutsOnDesktop"value="True"<property
name="DesktopDir"value="Citrix Applications">
```

> **Importante**
>
> En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen. Para obtener más información, consulte la documentación de StoreFront.

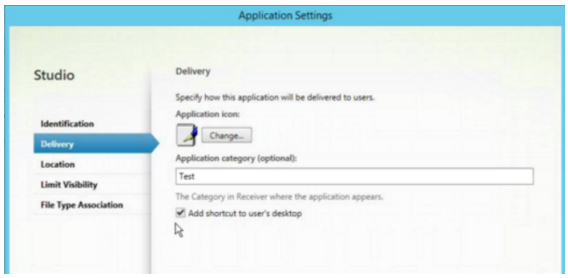
### Usar parámetros por aplicación en Citrix Virtual Apps and Desktops 7.x para personalizar ubicaciones de los accesos directos de las aplicaciones

La aplicación Citrix Workspace puede configurarse para que coloque automáticamente los accesos directos de los escritorios y las aplicaciones directamente en el menú Inicio o en el escritorio. Sin embargo, esta configuración es similar a la de las versiones anteriores de Workspace para Windows. Dicho esto, la versión 4.2.100 incorporó la capacidad de controlar la ubicación del acceso directo a la aplicación mediante los parámetros por aplicación de Citrix Virtual Apps. La función resulta útil en entornos donde hay varias aplicaciones que es necesario mostrar en ubicaciones coherentes.

### Usar parámetros por aplicación en XenApp 7.6 para personalizar las ubicaciones de los accesos directos de las aplicaciones

Para configurar un acceso directo de publicación para cada aplicación en XenApp 7.6:

1. En Citrix Studio, busque la pantalla **Parámetros de la aplicación**.
2. En la pantalla **Parámetros de la aplicación**, seleccione **Entrega**. En esta pantalla, puede especificar cómo se entregarán las aplicaciones a los usuarios.
3. Seleccione el icono adecuado para la aplicación. Haga clic en **Cambiar** para ir a la ubicación del icono necesario.
4. En el campo **Categoría de la aplicación**, opcionalmente, puede especificar la categoría en que aparece la aplicación dentro de Citrix Workspace. Por ejemplo, si está agregando accesos directos a aplicaciones de Microsoft Office, escriba Microsoft Office.
5. Marque la casilla “Agregar acceso directo al escritorio del usuario”.
6. Haga clic en Aceptar.




### Disminuir las demoras de enumeración o firma digital de código auxiliar de aplicaciones

La aplicación Citrix Workspace proporciona la funcionalidad para copiar los códigos auxiliares EXE de un recurso compartido de red si:

- Hay una demora en la enumeración de aplicaciones en cada inicio de sesión
- O es necesario firmar digitalmente los códigos auxiliares de las aplicaciones

Esta funcionalidad requiere varios pasos a seguir:

1. Cree el código auxiliar de cada aplicación en la máquina cliente.
2. Copie el código auxiliar de las aplicaciones en una ubicación común, accesible desde un recurso compartido de red.
3. Si es necesario, prepare una lista de permitidos o firme el código auxiliar con un certificado de empresa.
4. Agregue una clave de Registro para dejar que Citrix Workspace para Windows cree el código auxiliar copiándolo desde el recurso compartido de red.

Si **RemoveappsOnLogoff** y **RemoveAppsonExit** están habilitados, y los usuarios notan demoras en la enumeración de aplicaciones cada vez que inician una sesión, use la siguiente solución para reducir las demoras:

1. Use regedit para agregar `HKEY_CURRENT_USER\Software\Citrix\Dazzle` /v ReuseStubs /t REG_SZ /d “true”.
2. Use regedit para agregar `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle` /v ReuseStubs /t REG_SZ /d “true”. HKEY_CURRENT_USER prevalece sobre HKEY_LOCAL_MACHINE.

> **Precaución**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Permita que una máquina use archivos ejecutables de código auxiliar almacenados en el recurso compartido de red:

1. En una máquina cliente cree ejecutables de código auxiliar para todas las aplicaciones. Para crear ejecutables de código auxiliar, agregue todas las aplicaciones a la máquina mediante la aplicación Citrix Workspace; esta aplicación genera los archivos ejecutables.
2. Reúna los ejecutables de código auxiliar de `%APPDATA%\Citrix\SelfService`. Solamente necesita los archivos EXE.
3. Copie los archivos ejecutables a un recurso compartido de red.
4. Para cada máquina cliente que está bloqueada, establezca las siguientes claves de Registro:
   a) Reg add `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle` /v CommonStubDirectory /t REG_SZ /d “\\ShareOne\WorkspaceStubs”
   b) Reg add `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle` /v
   c) `CopyStubsFromCommonStubDirectory` /t REG_SZ /d “true”. También es posible configurar estos parámetros en HKEY_CURRENT_USER, si lo prefiere. HKEY_CURRENT_USER prevalece sobre HKEY_LOCAL_MACHINE.
   d) Salga de la aplicación Citrix Workspace y reiníciela para que los cambios surtan efecto.

**Ejemplo de casos de uso:**

Este tema proporciona casos de uso para los accesos directos de aplicaciones.

**Permitir a los usuarios elegir lo que quieran ver en el menú Inicio (Autoservicio)**

Si tiene docenas o incluso cientos de aplicaciones, permita a los usuarios seleccionar las aplicaciones para agregarlas al menú **Favoritos** e **Inicio**:

| | |
|---|---|
| Si quiere que el usuario elija las aplicaciones que quiera tener en su menú Inicio. | Configure la aplicación Citrix Workspace en el modo de autoservicio. En este modo, también deberá configurar los parámetros de palabra clave *auto* (aprovisionada automáticamente) y *mandatory* (obligatoria) para las aplicaciones, según sea necesario. |
| Si quiere que el usuario elija las aplicaciones que quiera colocar en su menú Inicio, pero también quiere colocar accesos directos específicos en el escritorio. | Configure la aplicación Citrix Workspace sin opciones y, a continuación, use parámetros para cada una de las aplicaciones que quiera mostrar en el escritorio. Use aplicaciones aprovisionadas automáticamente (*auto*) y obligatorias (*mandatory*), según sea necesario. |

**Menú Inicio sin accesos directos de aplicaciones**

Si el usuario utiliza un equipo doméstico que usa toda la familia, es posible que no sea necesario o conveniente colocar accesos directos. En tales casos, lo más sencillo es usar el acceso por explorador web; instale la aplicación Citrix Workspace sin configuración alguna y vaya a Citrix Workspace para Web. También puede configurar la aplicación Citrix Workspace para el acceso de autoservicio sin colocar accesos directos en ningún lugar.

| | |
|---|---|
| Si quiere evitar que la aplicación Citrix Workspace coloque accesos directos de aplicaciones en el menú Inicio automáticamente. | Configure la aplicación Citrix Workspace con PutShortcutsInStartMenu=False. La aplicación Citrix Workspace no coloca aplicaciones en el menú Inicio, ni siquiera en el modo de autoservicio, a menos que usted las coloque mediante los parámetros de cada aplicación. |

**Todos los accesos directos de aplicaciones en el menú Inicio o en el escritorio**

Si el usuario tiene pocas aplicaciones, coloque todas en el menú Inicio o en el escritorio, o bien en una carpeta del escritorio.

| | |
|---|---|
| Si quiere que la aplicación Citrix Workspace coloque todos los accesos directos de las aplicaciones en el menú Inicio automáticamente. | Configure la aplicación Citrix Workspace con SelfServiceMode=False. Todas las aplicaciones disponibles aparecen en el menú Inicio. |
| Si quiere que se coloquen accesos directos de todas las aplicaciones en el escritorio. | Configure la aplicación Citrix Workspace con PutShortcutsOnDesktop = true. Todas las aplicaciones disponibles aparecen en el escritorio. |
| Si quiere que todos los accesos directos se coloquen dentro de una carpeta en el escritorio. | Configure la aplicación Citrix Workspace con DesktopDir=Nombre de la carpeta de escritorio donde quiera las aplicaciones. |

**Parámetros por aplicación en XenApp 6.5 o 7.x**

Si quiere establecer la ubicación de los accesos directos de modo que cada usuario las encuentre en el mismo lugar, use los parámetros de aplicación de XenApp:

| | |
|---|---|
| Si quiere usar parámetros por aplicación para determinar dónde se colocarán las aplicaciones, independientemente de si se usa el modo de autoservicio o el modo de menú Inicio. | Configure la aplicación Citrix Workspace con PutShortcutsInStartMenu=false y habilite los parámetros por aplicación. |

**Aplicaciones en carpetas de categorías o en carpetas específicas**

Si quiere mostrar las aplicaciones en carpetas específicas, use las siguientes opciones:

| | |
|---|---|
| Si quiere que los accesos directos de las aplicaciones que la aplicación Citrix Workspace coloca en el menú Inicio aparezcan en su categoría (carpeta) asociada. | Configure la aplicación Citrix Workspace con UseCategoryAsStartMenuPath=True. |
| Si quiere que las aplicaciones que la aplicación Citrix Workspace coloca en el menú Inicio aparezcan en una carpeta específica: | Configure la aplicación Citrix Workspace con StartMenuDir=el nombre de la carpeta del menú Inicio. |

**Quitar aplicaciones al cerrar la sesión o al salir**

Si no quiere que los usuarios vean aplicaciones mientras otro usuario comparte el dispositivo de punto final, puede quitarlas cuando el usuario cierre sesión y salga.

| | |
|---|---|
| Si quiere que la aplicación Citrix Workspace quite todas las aplicaciones al cerrar sesión. | Configure la aplicación Citrix Workspace con RemoveAppsOnLogoff=True. |
| Si quiere que la aplicación Citrix Workspace quite las aplicaciones al salir. | Configure la aplicación Citrix Workspace con RemoveAppsOnExit=True. |

**Configurar aplicaciones para el acceso a aplicaciones locales**

Al configurar aplicaciones para el acceso a aplicaciones locales:

- Para especificar que se debe usar una aplicación instalada localmente en lugar de una

aplicación disponible en la aplicación Citrix Workspace, agregue la cadena de texto KEYWORDS:prefer=”pattern”. Esta función se conoce como Acceso a aplicaciones locales.

Antes de instalar una aplicación en el equipo de un usuario, la aplicación Citrix Workspace busca los patrones especificados para ver si la aplicación está instalada localmente. Si lo está, la aplicación Citrix Workspace se suscribe a la aplicación y no crea ningún acceso directo. Cuando el usuario inicia la aplicación desde la ventana de la aplicación Citrix Workspace, la aplicación Citrix Workspace inicia la aplicación instalada localmente (preferida).

Si un usuario desinstala una aplicación preferida desde fuera de la aplicación Citrix Workspace, la próxima vez que la aplicación Citrix Workspace se actualice, cancelará la suscripción a la aplicación. Si un usuario desinstala una aplicación preferida desde el cuadro de diálogo de la aplicación Citrix Workspace, la aplicación Citrix Workspace cancela la suscripción a la aplicación, pero no la desinstala.

> **Nota:**
>
> La palabra clave “prefer” se aplica cuando la aplicación Citrix Workspace se suscribe a una aplicación. Si se agrega la palabra clave después de haberse suscrito a la aplicación, esto no tiene efecto alguno.

Puede especificar la palabra clave prefer varias veces para una aplicación. Solo se necesita una vez para aplicar la palabra clave a una aplicación. Estos patrones pueden usarse en cualquier combinación:

- Para especificar que se debe usar una aplicación instalada localmente en lugar de una aplicación disponible en la aplicación Citrix Workspace, agregue la cadena de texto KEYWORDS:prefer=”pattern”. Esta función se conoce como Acceso a aplicaciones locales.

  Antes de instalar una aplicación en el equipo de un usuario, la aplicación Citrix Workspace busca los patrones especificados para ver si la aplicación está instalada localmente. Si lo está, la aplicación Citrix Workspace se suscribe a la aplicación y no crea ningún acceso directo. Cuando el usuario inicia la aplicación desde el cuadro de diálogo de la aplicación Citrix Workspace, la aplicación Citrix Workspace inicia la aplicación instalada localmente (preferida).

  Si un usuario desinstala una aplicación preferida desde fuera de la aplicación Citrix Workspace, la próxima vez que la aplicación Citrix Workspace se actualice, cancelará la suscripción a la aplicación. Si un usuario desinstala una aplicación preferida desde la aplicación Citrix Workspace, la aplicación Citrix Workspace cancela la suscripción a la aplicación, pero no la desinstala.

> **Nota:**
>
> La palabra clave “prefer” se aplica cuando la aplicación Citrix Workspace se suscribe a una aplicación. Si se agrega la palabra clave después de haberse suscrito a la aplicación, esto no tiene efecto alguno.

Puede especificar la palabra clave prefer varias veces para una aplicación. Solo se necesita una vez para aplicar la palabra clave a una aplicación. Estos patrones pueden usarse en cualquier combinación:

- prefer="NombreDeAplicación"

  El patrón del nombre de la aplicación hará coincidir cualquier aplicación que contenga dicho nombre en el nombre del archivo de acceso directo. El nombre de aplicación puede ser una palabra o una frase. Para introducir frases hay que usar comillas. No se hacen coincidir palabras o rutas de archivo incompletas, y la coincidencia no distingue entre mayúsculas y minúsculas. El patrón de coincidencia de nombre de aplicación resulta útil para sobrescritura de parámetros realizadas manualmente por un administrador.

| KEYWORDS:prefer= | Acceso directo en Programas | ¿Coincide? |
|---|---|---|
| Word | \Microsoft Office\Microsoft Word 2010 | Sí |
| Microsoft Word | \Microsoft Office\Microsoft Word 2010 | Sí |
| Consola | McAfee\VirusScan Console | Sí |
| Virus | McAfee\VirusScan Console | No |
| Consola | McAfee\VirusScan Console | Sí |

- prefer="\\Carpeta1\Carpeta2\…\NombreDeAplicación"

  El patrón de la ruta absoluta coincide con la ruta completa del archivo de acceso directo, además del nombre completo de la aplicación en el menú Inicio. La carpeta Programas es una subcarpeta del directorio del menú Inicio, de modo que hay que incluirla en la ruta absoluta si el destino es una aplicación de esa carpeta. Si la ruta contiene espacios hay que usar comillas. La coincidencia distingue entre mayúsculas y minúsculas. El patrón de coincidencia de la ruta absoluta es útil para sobrescrituras implementadas mediante programación en Citrix Virtual Apps and Desktops y Citrix DaaS.

| KEYWORDS:prefer= | Acceso directo en Programas | ¿Coincide? |
|---|---|---|
| \Programs\Microsoft Office\Microsoft Word 2010 | \Programs\Microsoft Office\Microsoft Word 2010 | Sí |
| \Microsoft Office | \Programs\Microsoft Office\Microsoft Word 2010 | No |
| \Microsoft Word 2010 | \Programs\Microsoft Office\Microsoft Word 2010 | No |

| KEYWORDS:prefer= | Acceso directo en Programas | ¿Coincide? |
|---|---|---|
| \Programs\Microsoft Word 2010 | \Programs\Microsoft Word 2010 | Sí |

- prefer="\Carpeta1\Carpeta2\…\NombreDeAplicación"

  El patrón de la ruta relativa coincide con la ruta relativa del archivo de acceso directo en el menú Inicio. La ruta relativa suministrada debe contener el nombre de la aplicación y puede, de manera optativa, incluir las carpetas donde reside el acceso directo. La coincidencia es correcta si la ruta del archivo de acceso directo termina con la ruta relativa suministrada. Si la ruta contiene espacios hay que usar comillas. La coincidencia distingue entre mayúsculas y minúsculas. El patrón de coincidencia de la ruta absoluta es útil para sobrescrituras implementadas mediante programación.

| KEYWORDS:prefer= | Acceso directo en Programas | ¿Coincide? |
|---|---|---|
| \Microsoft Office\Microsoft Word 2010 | \Microsoft Office\Microsoft Word 2010 | Sí |
| \Microsoft Office | \Microsoft Office\Microsoft Word 2010 | No |
| \Microsoft Word 2010 | \Microsoft Office\Microsoft Word 2010 | Sí |
| \Microsoft Word | \Microsoft Word 2010 | No |

Para obtener más información sobre otras palabras clave, consulte "Recomendaciones adicionales" en Optimizar la experiencia de usuario, en la documentación de StoreFront.

### Distribución de pantallas virtuales

Esta función le permite definir una distribución de monitores virtuales que se aplica al escritorio remoto. También puede dividir un único monitor de cliente virtualmente en un máximo de ocho monitores en el escritorio remoto. Puede configurar los monitores virtuales en la ficha **Distribución del monitor** en Desktop Viewer. Allí, puede dibujar líneas horizontales o verticales para separar la pantalla en monitores virtuales. La pantalla se divide en función de porcentajes especificados en la resolución del monitor cliente.

Puede establecer los PPP en los monitores virtuales que se utilizarán para el escalado de PPP o la correspondencia de PPP. Después de aplicar una distribución de monitores virtuales, cambie el tamaño o vuelva a conectarse a la sesión.

Esta configuración se aplica solo a las sesiones de escritorio de un solo monitor y en pantalla completa, no afecta a ninguna aplicación publicada. Esta configuración se aplica a todas las conexiones posteriores de ese cliente.

A partir de Citrix Workspace para Windows 2106, la distribución de pantallas virtuales también está disponible en sesiones de escritorio de pantalla completa y con varios monitores. La distribución de pantallas virtuales está habilitada de forma predeterminada. En casos con varios monitores, se aplica la misma distribución de pantallas virtuales configurada a todos los monitores de la sesión si el total de pantallas virtuales no es superior a ocho pantallas virtuales. Si se supera este límite, la distribución de pantallas virtuales se ignora y no se aplica a ningún monitor de la sesión.

Para inhabilitar la mejora para varios monitores, configure esta clave del Registro:

- `HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer`

Nombre: **SplitAllMonitors**
Tipo: DWORD

Valores:

1: Habilitada

0: Inhabilitada

### Tiempo de inicio de las aplicaciones

La función de preinicio de sesiones permite reducir el tiempo que tardan en abrirse las aplicaciones durante los períodos de mucho tráfico o tráfico normal, mejorando así la experiencia del usuario. La función de preinicio permite crear una sesión de preinicio. La sesión de preinicio se crea cuando un usuario inicia sesión en la aplicación Citrix Workspace o a una hora programada si el usuario ha iniciado sesión.

La sesión de preinicio reduce el tiempo que tarda en iniciarse la primera aplicación. Cuando un usuario agrega una nueva conexión de cuenta a la aplicación Citrix Workspace para Windows, el preinicio de sesiones no surte efecto hasta la siguiente sesión. La aplicación predeterminada ctxprelaunch.exe se ejecuta en esta sesión, pero no es visible.

Para obtener más información, consulte las instrucciones para el preinicio de sesiones y la persistencia de sesiones en el artículo de Citrix Virtual Apps and Desktops titulado Administrar grupos de entrega.

El preinicio de sesiones está inhabilitado de forma predeterminada. Para habilitar el preinicio de sesiones, especifique el parámetro `ENABLEPRELAUNCH=true` en la línea de comandos de Workspace o establezca la clave de Registro `EnablePreLaunch` en true. El parámetro predeterminado es Null y significa que el preinicio está inhabilitado.

> **Nota:**
>
> Si la máquina cliente se ha configurado para admitir la autenticación PassThrough de dominio (SSON), el preinicio está habilitado automáticamente. Si quiere usar la autenticación PassThrough de dominio (Single Sign-On) sin la función de preinicio, establezca el valor de la clave de Registro **EnablePreLaunch** en
> false.

Las ubicaciones en el Registro son:

- `HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\\Dazzle`
- `HKEY_CURRENT_USER\Software\Citrix\Dazzle`

Existen dos tipos de preinicio:

- **Preinicio a petición:** El preinicio se lleva a cabo inmediatamente después de autenticarse las credenciales del usuario, independientemente del tráfico de la red. Por lo general, se usa en períodos de tráfico normal. Un usuario puede provocar el preinicio si reinicia la aplicación Citrix Workspace.
- **Preinicio programado:** El preinicio ocurre a una hora programada. El preinicio programado ocurre solamente cuando el dispositivo de usuario ya se está ejecutando y se ha autenticado. Si no se cumplen estas dos condiciones cuando llega la hora del preinicio programado, no se inicia la sesión. La sesión se inicia en una ventana a la hora programada lo que permite compartir la carga de red y del servidor. Por ejemplo, si el preinicio programado está programado para las 13:45, la sesión se inicia realmente entre las 13:15 y las 13:45. Por lo general, se usa en períodos de mucho tráfico.

La configuración del preinicio en un servidor de Citrix Virtual Apps consiste en lo siguiente:

- Crear, modificar o eliminar aplicaciones de preinicio
- Y actualizar los parámetros de directivas de usuario que controlan la aplicación de preinicio

No se puede usar el archivo `receiver.admx` para personalizar la función de preinicio. Sin embargo, puede cambiar la configuración de preinicio al modificar valores del Registro. Los valores del Registro se pueden modificar durante o después de la instalación de la aplicación Citrix Workspace para Windows.

- Los valores HKEY_LOCAL_MACHINE se escriben durante la instalación del cliente.
- Los valores HKEY_CURRENT_USER permiten dar diferentes parámetros a los distintos usuarios de una misma máquina. Los usuarios pueden cambiar los valores HKEY_CURRENT_USER sin necesidad de permisos de administrador. Puede proporcionar a sus usuarios scripts para cambiar los valores.

**Valores de Registro HKEY_LOCAL_MACHINE:**

Para sistemas operativos Windows de 64 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Prelaunch`

Para sistemas operativos Windows de 32 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Prelaunch`

Nombre: **UserOverride**
Tipo: REG_DWORD

Valores:

0: Usa los valores de HKEY_LOCAL_MACHINE, incluso si ya existen valores de HKEY_CURRENT_USER.

1: Usa los valores de HKEY_CURRENT_USER si ya existen; de lo contrario, usa los valores de HKEY_LOCAL_MACHINE.

Nombre: **State**
Tipo: REG_DWORD

Valores:

0: Inhabilita el preinicio.

1: Habilita el preinicio a petición (el preinicio comienza después de autenticar las credenciales del usuario).

2: Habilita el preinicio programado (el preinicio comienza a la hora configurada en Schedule).

Nombre: **Schedule**
Tipo: REG_DWORD

Valor:

Hora (en formato de 24 horas) y días de la semana para los preinicios programados, con este formato:

| | | |
|---|---|---|
| HH:MM | M:T:W:TH:F:S:SU, donde HH y MM son las horas y los minutos. M:T:W:TH:F:S:SU son los días de la semana. Por ejemplo, para habilitar el preinicio programado los lunes, miércoles y viernes a las 13:45, configure Schedule en Schedule=13:45 | 1:0:1:0:1:0:0. La sesión se inicia entre las 13:15 y las 13:45. |

**Valores de Registro HKEY_CURRENT_USER:**

`HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Prelaunch`

Las claves **State** y **Schedule** tienen los mismos valores que para HKEY_LOCAL_MACHINE.

### Redirección bidireccional de contenido

La directiva "Redirección bidireccional de contenido" permite habilitar o inhabilitar la redirección de direcciones URL entre el host y el cliente y viceversa. Las directivas de servidor se configuran en Citrix Studio, y las directivas de cliente se configuran en la plantilla administrativa de objetos de directiva de grupo de la aplicación Citrix Workspace.

Citrix ofrece redirección de host a cliente y acceso a aplicaciones locales para la redirección de cliente a URL. Sin embargo, recomendamos utilizar redirección bidireccional de contenido para los clientes de Windows que se unen a un dominio.

Es posible habilitar la redirección bidireccional de contenido mediante uno de los siguientes métodos:

1. Plantilla administrativa de objetos de directiva de grupo (GPO)
2. Editor del Registro

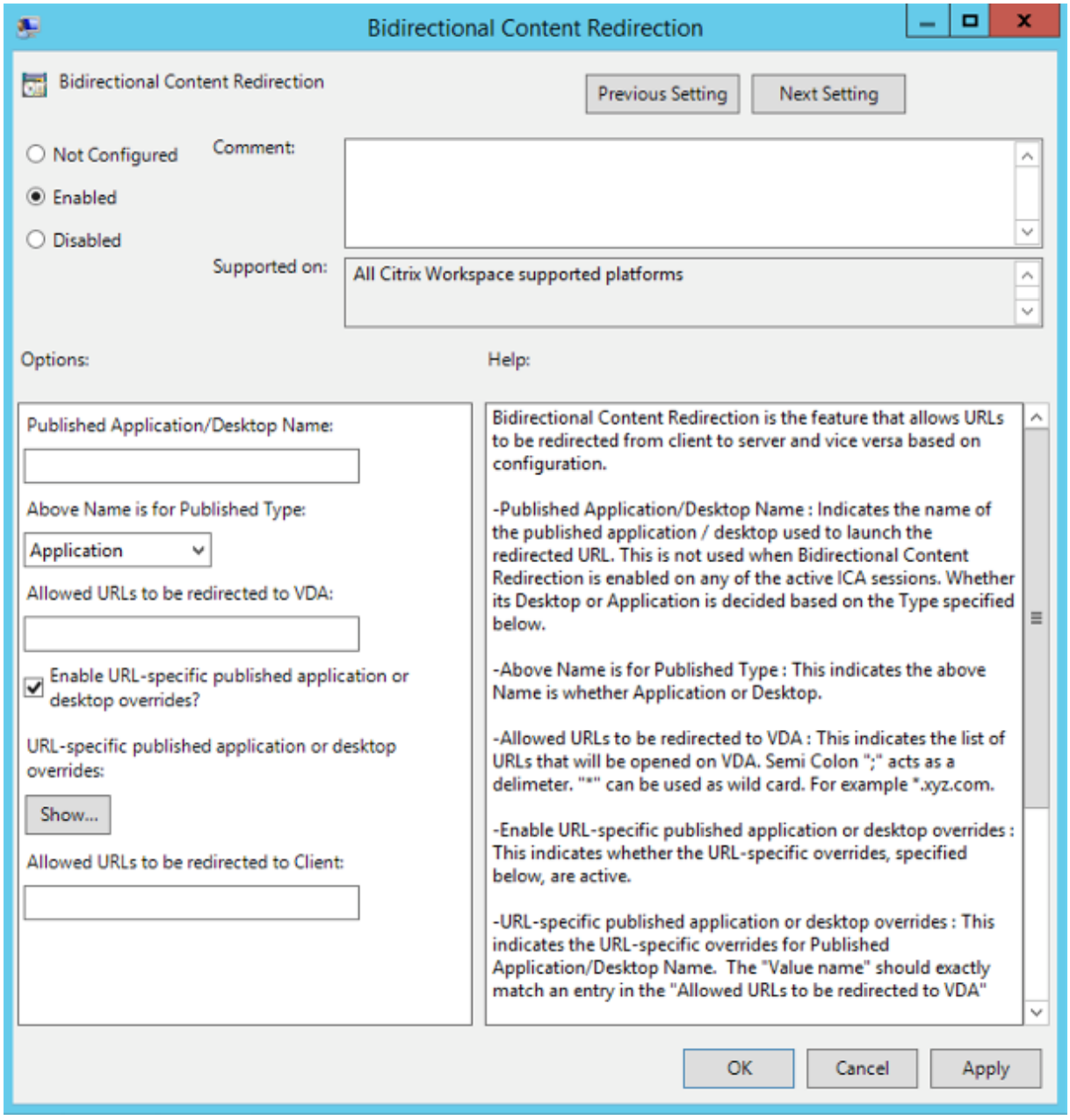
> **Nota:**
>
> - La redirección bidireccional de contenido no funciona en las sesiones donde está habilitado el **Acceso a aplicaciones locales**.
> - La redirección bidireccional de contenido debe estar habilitada tanto en el servidor como en el cliente. Cuando esté inhabilitada en alguna de las partes, ya sea el servidor o el cliente, la funcionalidad estará inhabilitada.
> - Al incluir direcciones URL, puede especificar una sola dirección URL o una lista de direcciones URL, delimitadas por punto y coma. Puede utilizar un asterisco (*) como comodín.

**Para habilitar la redirección bidireccional de contenido mediante la plantilla administrativa de GPO:**

Use la configuración de la plantilla administrativa de GPO solo para la primera instalación de la aplicación Citrix Workspace para Windows.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del usuario**, vaya a **Plantillas administrativas** > **Plantillas administrativas clásicas (ADM)** > **Componentes de Citrix** > **Citrix Workspace** > **Experiencia de usuario**.
3. Seleccione la directiva **Redirección bidireccional de contenido**.




1. En el campo **Nombre de aplicación o escritorio publicados**, indique el nombre del recurso utilizado para iniciar la dirección URL redirigida.

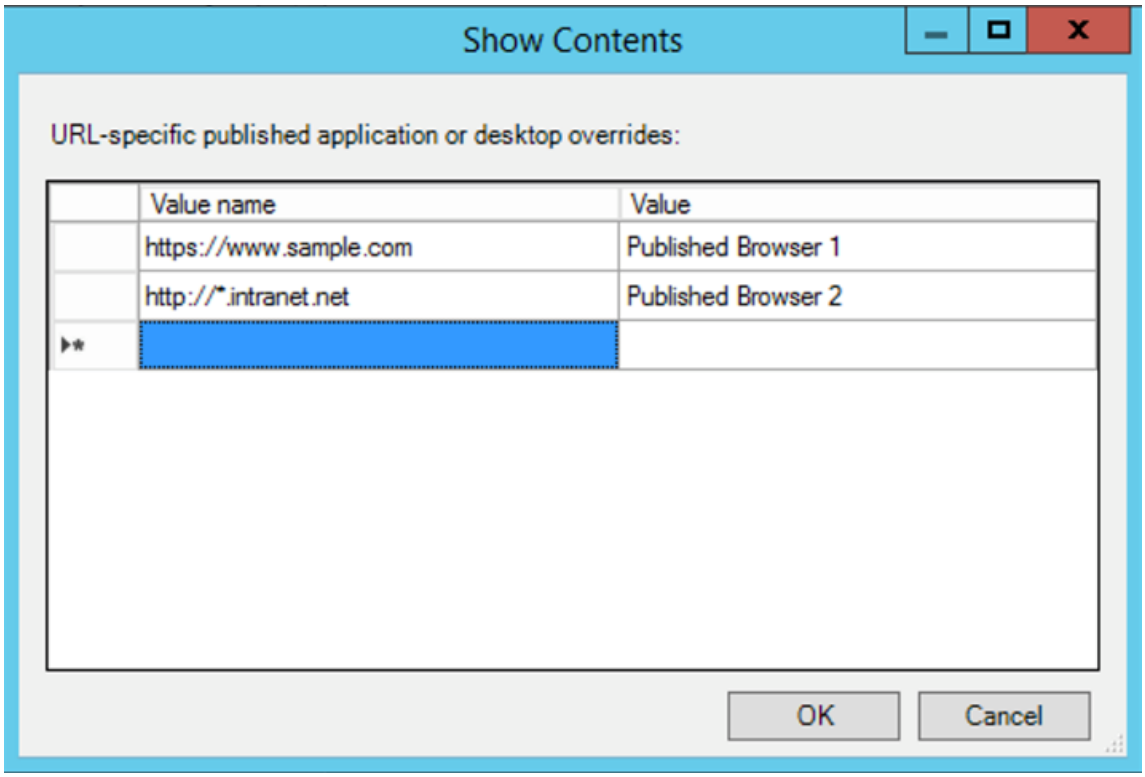
   > **Nota:**
   >
   > Al incluir direcciones URL, especifique una sola dirección URL o una lista de direcciones URL, delimitadas por punto y coma. Puede utilizar un asterisco (*) como comodín.

2. En **Tipo de recurso publicado**, seleccione **Aplicación** o **Escritorio** del recurso según corresponda.
3. En el campo **Direcciones URL permitidas para redirigir al VDA**, introduzca las direcciones URL

que se deben redirigir. Separe cada dirección de la lista con un punto y coma.

4. Seleccione la opción **Habilitar el reemplazo de aplicaciones o escritorios publicados con direcciones URL específicas** para supeditar una URL.
5. Haga clic en **Mostrar** para ver una lista en la que el nombre del valor debe coincidir con cualquiera de las direcciones URL indicadas en el campo **Direcciones URL permitidas para redirigir al VDA**. El valor debe coincidir con el nombre de una aplicación publicada.




6. En el campo **Direcciones URL permitidas para redirigir al cliente**, introduzca las direcciones URL que se deben redirigir del servidor al cliente. Separe cada dirección de la lista con un punto y coma.

   > **Nota:**
   >
   > Al incluir direcciones URL, especifique una sola dirección URL o una lista de direcciones URL, delimitadas por punto y coma. Puede utilizar un asterisco (*) como comodín.

7. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**
8. Desde la línea de comandos, ejecute el comando `gpupdate /force`.

**Para habilitar la redirección bidireccional de contenido mediante el Registro:**

Para habilitar la redirección bidireccional de contenido, ejecute el comando `redirector.exe /RegIE` en el cliente de la aplicación Citrix Workspace y desde la carpeta de instalación de la aplicación Citrix Workspace: `C:\Program Files (x86)\Citrix\ICA Client`).

**Importante:**

- Compruebe que la regla de redirección no resulta en un bucle. Cuando las reglas del VDA se definen para que la URL `https://www.my\\_company.com` se redirija, por ejemplo, al cliente y también para que la misma URL se redirija al VDA, el resultado es un bucle.
- La función de redirección de URL solo admite direcciones URL explícitas (aquellas que aparecen en la barra de direcciones del explorador o las que se encuentran navegando dentro del explorador, según el explorador que se esté usando).
- Si hay dos aplicaciones con el mismo nombre simplificado que usan varias cuentas de StoreFront, el nombre simplificado de la cuenta principal de StoreFront se utiliza para iniciar la aplicación o una sesión de escritorio.
- Solo se abre una nueva ventana de explorador web cuando una dirección URL se redirige al cliente. Cuando una dirección URL se redirige al VDA, si el explorador web ya está abierto, la URL redirigida se abre en una nueva ficha.
- Se admiten enlaces incrustados en archivos como documentos, mensajes de correo electrónico y archivos PDF.
- Compruebe que, en una máquina, hay habilitada una de las directivas de redirección de contenido del host y solamente existe una de las asociaciones de tipos de archivo de servidor. Citrix recomienda inhabilitar la asociación de tipos de archivo de servidor o la función de redirección de contenido de host (URL) para confirmar que la redirección de URL funciona correctamente.
- En Internet Explorer, haga clic en **Configuración** > **Opciones de Internet** > **Avanzado** y marque la casilla **Habilitar extensiones de explorador de terceros** en la sección **Exploración**.

**Limitación:**

Si la redirección falla debido a problemas de lanzamiento de la sesión, no hay ningún mecanismo alternativo.

### Función de URL bidireccionales con exploradores web basados en Chromium

La redirección bidireccional de contenido permite configurar direcciones URL para redirigir contenido del cliente al servidor y del servidor al cliente mediante directivas en el servidor y en el cliente.

Las directivas de servidor se establecen en el Delivery Controller, y las directivas de cliente se establecen en la aplicación Citrix Workspace. Las directivas se establecen mediante la plantilla administrativa de objetos de directiva de grupo (GPO).

A partir de la versión 2106, se ofrece la redirección bidireccional de URL para Google Chrome y Microsoft Edge.

**Requisitos previos:**

- Citrix Virtual Apps and Desktops 2106 o una versión posterior.
- Versión 5.0 de la extensión de redirección del explorador web.

Para registrar el explorador web Google Chrome en la redirección bidireccional de URL, ejecute este comando desde la carpeta de instalación de la aplicación Citrix Workspace:

```
%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regChrome /verbose
```

> **Nota:**
>
> Al utilizar estos comandos en exploradores Chrome, la extensión de redirección de contenido bidireccional se instala automáticamente desde Chrome Web Store.

Para cancelar el registro del explorador web Google Chrome de la redirección bidireccional de URL, ejecute este comando desde la carpeta de instalación de la aplicación Citrix Workspace:

```
%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregChrome /verbose
```

> **Nota:**
>
> Si aparece este error al acceder a la página Extensiones del explorador web, ignórelo:
>
> ```
> Websocket connection to wss://... failed.
> ```

Para obtener información sobre cómo configurar la redirección de URL en la aplicación Citrix Workspace, consulte Redirección de contenido bidireccional.

Para obtener más información sobre la redirección de contenido del explorador web, consulte Redirección de contenido de explorador web en la documentación de Citrix Virtual Apps and Desktops.

**Para impedir que la ventana de Desktop Viewer se atenúe:**

Si utiliza varias ventanas de Desktop Viewer, de manera predeterminada se atenúan los escritorios que no están activos. Si los usuarios quieren ver varios escritorios simultáneamente, es posible que la información que contienen no sea legible. Para inhabilitar el comportamiento predeterminado e impedir que la ventana de **Desktop Viewer** se atenúe, modifique el Editor del Registro.

> **Precaución**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

- En el dispositivo de usuario, cree una entrada de Registro REG_DWORD denominada **DisableDimming** en una de las siguientes claves, dependiendo de si quiere impedir la atenuación solo para el usuario actual del dispositivo, o para el dispositivo propiamente dicho. Existe un registro si Desktop Viewer se ha utilizado en el dispositivo:

- HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer
- HKEY_LOCAL_MACHINE\Software\Citrix\XenDesktop\DesktopViewer

O bien, en lugar de controlar la atenuación, puede definir una directiva local creando la misma entrada REG_WORD en una de las siguientes claves:

- HKEY_CURRENT_USER\Software\Policies\Citrix\XenDesktop\DesktopViewer
- HKEY_LOCAL_MACHINE\Software\Policies\Citrix\XenDesktop\DesktopViewer

Antes de utilizar estas claves, compruebe si el administrador de Citrix Virtual Apps and Desktops y Citrix DaaS ha establecido una directiva para esta función.

Establezca la entrada en cualquier valor distinto de cero, como 1 o true (verdadero).

Si no se especifican entradas o si esta se establece en 0, la ventana de **Desktop Viewer** se atenúa. Si se especifican varios registros, se utiliza la siguiente prioridad. El primer registro de esta lista y su valor determinan si la ventana se atenúa:

1. HKEY_CURRENT_USER\Software\Policies\Citrix\…
2. HKEY_LOCAL_MACHINE\Software\Policies\Citrix\…
3. HKEY_CURRENT_USER\Software\Citrix\…
4. HKEY_LOCAL_MACHINE\Software\Citrix\…

### Citrix Casting

Citrix Ready Workspace Hub combina entornos digitales y físicos para entregar aplicaciones y datos dentro de un espacio inteligente y seguro. El sistema completo conecta dispositivos (o cosas), como aplicaciones móviles y sensores, para crear un entorno inteligente que responda adecuadamente.

Citrix Ready Workspace Hub se ha construido sobre la plataforma Raspberry Pi 3. El dispositivo que ejecuta la aplicación Citrix Workspace se conecta a Citrix Ready Workspace Hub y transmite las aplicaciones o los escritorios hacia una pantalla más grande. Citrix Casting solo se admite en la versión 1607 de Microsoft Windows 10 y en versiones posteriores o en Windows Server 2016.

La función Citrix Casting permite acceder de forma instantánea y segura a cualquier aplicación desde un dispositivo móvil y mostrarla en una pantalla grande.

> **Nota:**
>
> - Citrix Casting para Windows admite la versión 2.40.3839 de Citrix Ready Workspace Hub y versiones posteriores. Es posible que las versiones anteriores de Citrix Ready Workspace Hub no se detecten o causen un error de proyección.
> - La función Citrix Casting no está disponible en la aplicación Citrix Workspace para Windows (Store).

**Requisitos previos:**

- Bluetooth está habilitado en el dispositivo para detectar hubs.
- Tanto Citrix Ready Workspace Hub como la aplicación Citrix Workspace deben estar en la misma red.
- El puerto 55555 está habilitado entre el dispositivo que ejecuta la aplicación Citrix Workspace y Citrix Ready Workspace Hub.
- Para Citrix Casting, el puerto 1494 no se debe bloquear.
- El puerto 55556 es el puerto predeterminado para las conexiones SSL entre los dispositivos móviles y Citrix Ready Workspace Hub. Puede configurar otro puerto SSL en la página de parámetros de Raspberry Pi. Si el puerto SSL está bloqueado, los usuarios no pueden establecer conexiones SSL con Workspace Hub.
- Citrix Casting solo se admite en la versión 1607 de Microsoft Windows 10 y en versiones posteriores o en Windows Server 2016.
- Ejecute el comando `/IncludeCitrixCasting` durante la instalación para habilitar Citrix Casting.

**Configurar el inicio de Citrix Casting**

> **Nota:**
>
> Puede ocultar toda o parte de la hoja Preferencias avanzadas. Para obtener más información, consulte Hoja de Preferencias avanzadas.

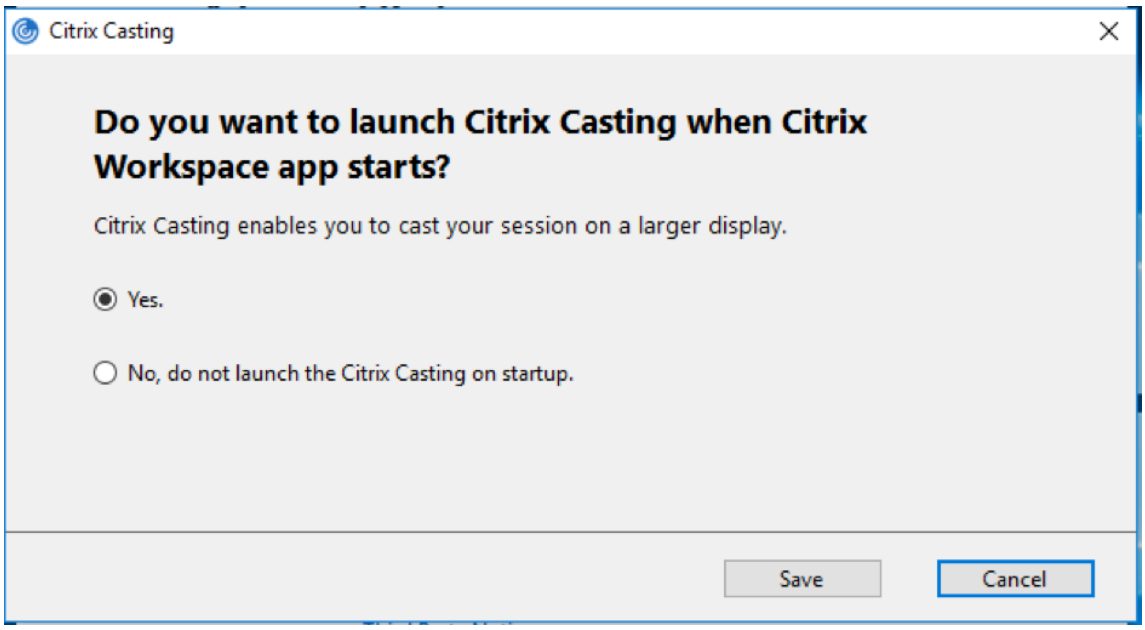
1. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace en el área de notificaciones y seleccione **Preferencias avanzadas**.

   Aparecerá el cuadro de diálogo **Preferencias avanzadas**.

2. Seleccione **Citrix Casting**.

   Aparece el cuadro de diálogo **Citrix Casting**.




3. Seleccione una de estas opciones:
   - Sí: Indica que Citrix Casting se inicia cuando se inicia la aplicación Citrix Workspace.
   - No, no abrir Citrix Casting al iniciar: Citrix Casting no se inicia cuando se inicia la aplicación Citrix Workspace.

   > **Nota:**
   >
   > Seleccionar la opción **No** no finaliza la sesión actual de proyección de pantalla. La configuración se aplica solo en el próximo inicio de la aplicación Citrix Workspace.

4. Haga clic en **Guardar** para aplicar los cambios.

#### Cómo usar Citrix Casting con la aplicación Citrix Workspace

1. Inicie sesión en la aplicación Citrix Workspace y active Bluetooth en el dispositivo.

   Se muestra la lista de hubs disponibles. La lista está ordenada por el valor RSSI del paquete de baliza de Workspace Hub.

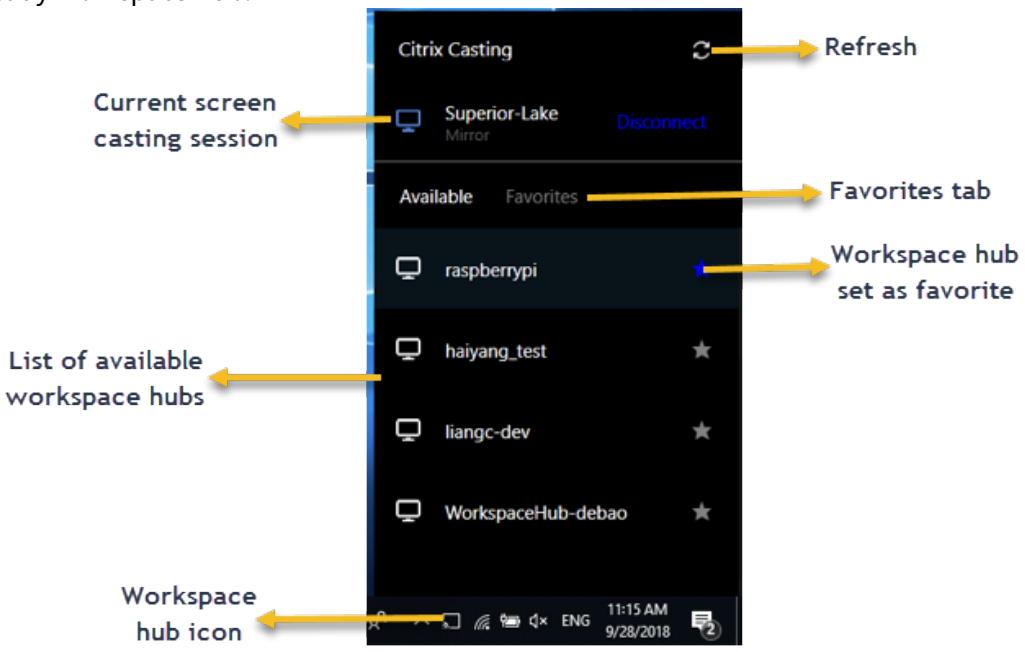
2. Seleccione el dispositivo Workspace Hub para proyectar su pantalla y elija una de las siguientes opciones:
   - **Mirror** (reflejar) para duplicar la pantalla principal y proyectarla en el dispositivo Workspace Hub conectado.
   - **Extend** (extender) para usar la pantalla del dispositivo Workspace Hub como pantalla secundaria.

> **Nota:**
>
> Salir de la aplicación Citrix Workspace no implica salir de Citrix Casting.

En el cuadro de diálogo de **notificación de Citrix Casting**, están disponibles las siguientes opciones:

1. La sesión de proyección de pantalla actual se muestra en la parte superior.
2. Icono de **actualización**.
3. **Desconectar** para detener la sesión de proyección de pantalla actual.
4. Icono con forma de estrella para agregar el Workspace Hub a los **favoritos**.
5. Haga clic con el botón secundario en el icono de Workspace Hub situado en el área de notificaciones y seleccione **Salir** para desconectar la sesión de proyección de pantalla y salir de Citrix Ready Workspace Hub.




### Lista de autocomprobación

Si la aplicación Citrix Workspace no puede detectar ni comunicarse con ningún Workspace Hub disponible dentro del alcance, debe llevar a cabo lo siguiente como parte de la autocomprobación:

1. La aplicación Citrix Workspace y Citrix Ready Workspace Hub están conectados a la misma red.
2. Bluetooth está habilitado y funciona correctamente en el dispositivo donde se ha iniciado la aplicación Citrix Workspace.
3. El dispositivo en el que se ha iniciado la aplicación Citrix Workspace se encuentra al alcance (a menos de 10 metros y sin ningún obstáculo, como paredes) de Citrix Ready Workspace Hub.
4. Inicie un explorador web en la aplicación Citrix Workspace y escriba `http://<hub_ip>:55555/device-details.xml` para comprobar si muestra datos del dispositivo Workspace

Hub.

5. Haga clic en el icono de **actualización** en Citrix Ready Workspace Hub e intente volver a conectarse al Workspace Hub.

#### Problemas conocidos y limitaciones

1. Citrix Casting no funciona a menos que el dispositivo esté conectado a la misma red que Citrix Ready Workspace Hub.
2. Si hay problemas de red, es posible que haya demoras en la pantalla del dispositivo Workspace Hub.
3. Cuando selecciona **Extender**, la pantalla principal donde esté iniciada la aplicación Citrix Ready Workspace parpadea varias veces.
4. En el modo **Extender**, no se puede configurar la pantalla secundaria como pantalla principal.
5. La sesión de proyección de pantalla se desconecta automáticamente cuando hay algún cambio en la configuración de visualización en el dispositivo. Por ejemplo, un cambio en la resolución de la pantalla o un cambio en la orientación de la pantalla.
6. Durante la sesión de proyección de pantalla, si el dispositivo que ejecuta la aplicación Citrix Workspace se bloquea, se suspende o hiberna, aparece un error al iniciar sesión.
7. No se admiten las sesiones de proyección en varias pantallas.
8. La resolución de pantalla máxima admitida por Citrix Casting es 1920 x 1440.
9. Citrix Casting admite la versión 2.40.3839 de Citrix Ready Workspace Hub y versiones posteriores. Es posible que las versiones anteriores de Citrix Ready Workspace Hub no se detecten o causen un error de proyección.
10. Esta función no se ofrece en la aplicación Citrix Workspace para la Tienda Windows.
11. Puede que Citrix Casting en modo **Extender** no esté posicionado correctamente en Windows 10, compilación 1607.

Para obtener más información sobre Citrix Ready Workspace Hub, consulte la sección Citrix Ready Workspace Hub en la documentación de Citrix Virtual Apps and Desktops.

### Escalado de PPP

La aplicación Citrix Workspace cuenta con reconocimiento de PPP y permite la correspondencia de resoluciones de pantalla y el escalado de PPP en el cliente Windows con la sesión de aplicaciones y escritorios virtuales.

El escalado de PPP se usa principalmente con monitores de gran tamaño y alta resolución para mostrar aplicaciones, texto, imágenes y otros elementos gráficos en un tamaño que se pueda ver cómodamente.

Esta función está habilitada de forma predeterminada y es el parámetro recomendado para todos los casos de uso. Sin embargo, los administradores pueden seguir configurando el escalado de PPP medi-

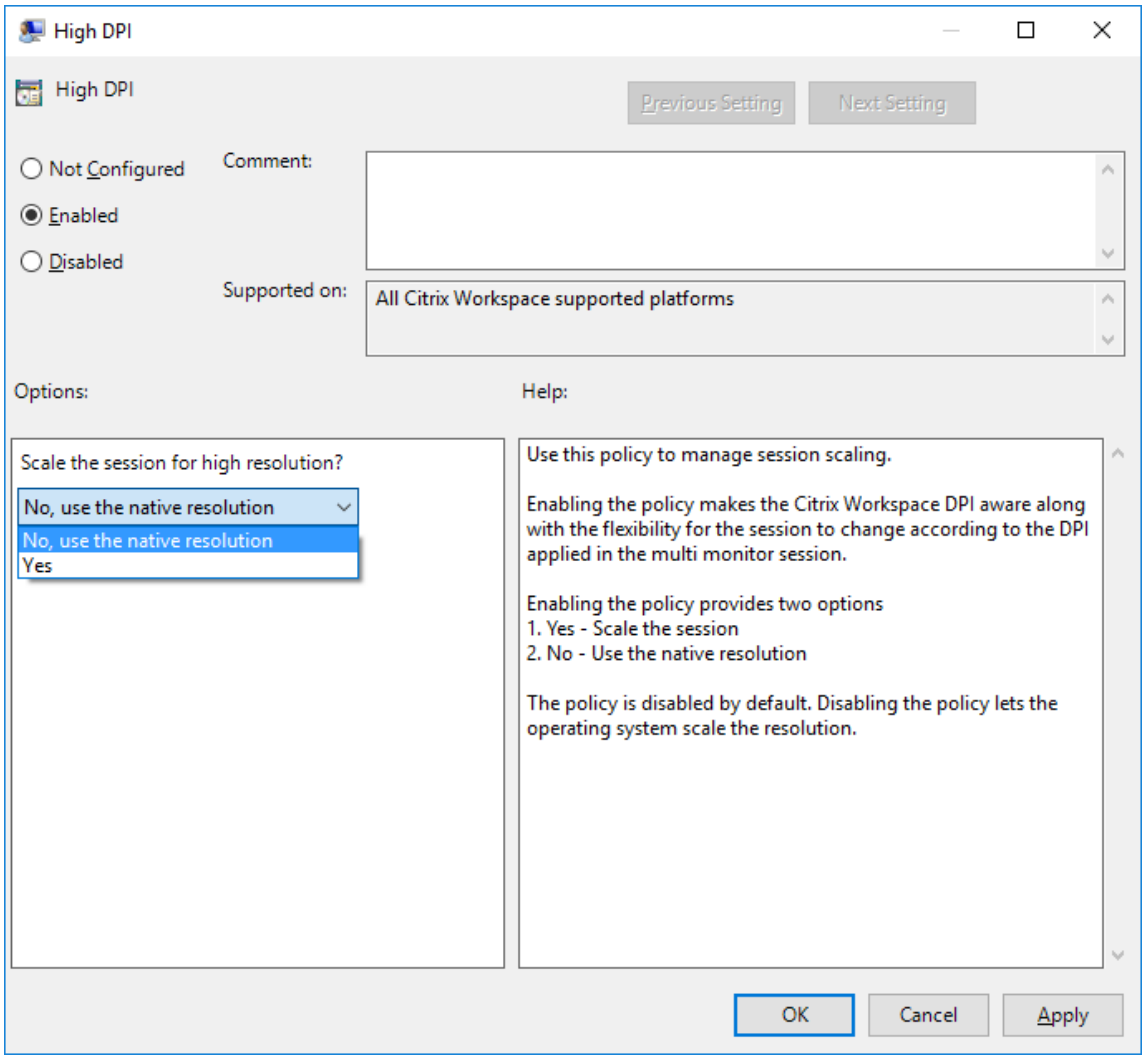
 

ante la plantilla administrativa de objeto de directiva de grupo, o GPO, (configuración por máquina), si es necesario.

Para configurar el ajuste de escala de PPP mediante la plantilla administrativa de GPO:

**Para configurar el ajuste de escala de PPP mediante la plantilla administrativa de GPO:**

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **PPP**.
3. Seleccione la directiva **PPP elevados**.




4. Seleccione una de estas opciones:
    a) Sí: Se aplican PPP elevados en una sesión.
    b) No, usar la resolución nativa: El sistema operativo se encarga de configurar la resolución.

5. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**
6. Desde la línea de comandos, ejecute el comando `gpupdate /force` para aplicar los cambios.

**Configurar el escalado de PPP mediante la interfaz gráfica de usuario:**

1. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace situado en el área de notificaciones.
2. Seleccione **Preferencias avanzadas** y haga clic en **PPP elevado**.
3. Seleccione una de estas opciones:
   a) **Sí**: Se aplican PPP elevados en una sesión.
   b) **No, usar la resolución nativa**: La aplicación Citrix Workspace detecta los PPP en el VDA y los aplica.
   c) **Dejar que el sistema operativo ajuste la resolución**: De forma predeterminada, está seleccionada esta opción. Permite a Windows encargarse del escalado de PPP. Esta opción también significa que se inhabilita la directiva PPP elevados.
4. Haga clic en **Guardar**.
5. Reinicie la sesión de la aplicación Citrix Workspace para que los cambios surtan efecto.

NOTA:

> **Consideraciones adicionales:**
>
> - La correspondencia de PPP requiere la versión 1912 LTSR de Citrix Virtual Apps and Desktops o una posterior.
> - En la mayoría de los casos, se recomienda el parámetro **No, usar la resolución nativa** (correspondencia de PPP).
> - El parámetro predeterminado **Dejar que el sistema operativo ajuste la resolución** inhabilita el reconocimiento de PPP en la aplicación Citrix Workspace. Es posible que este modo produzca gráficos borrosos cuando la escala de PPP del cliente Windows se establece en un valor distinto al 100 %. Este modo no admite varios monitores con diferentes escalas de PPP.
> - La opción **Sí** hace que la aplicación Citrix Workspace amplíe la escala de la ventana de la sesión para que coincida con la escala de PPP configurada en el cliente Windows. Se trata de una función antigua que se recomienda solo para conexiones a entornos antiguos de XenApp y XenDesktop cuando se requieren escalas de PPP superiores al 100 % en el cliente. Es posible que este modo produzca gráficos borrosos.

Para obtener información sobre la solución de problemas de escalado de PPP, consulte el artículo CTX230017 de Knowledge Center.

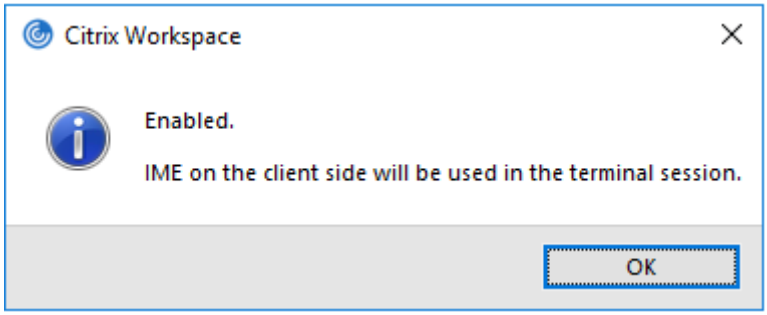
### Editores IME de cliente genérico

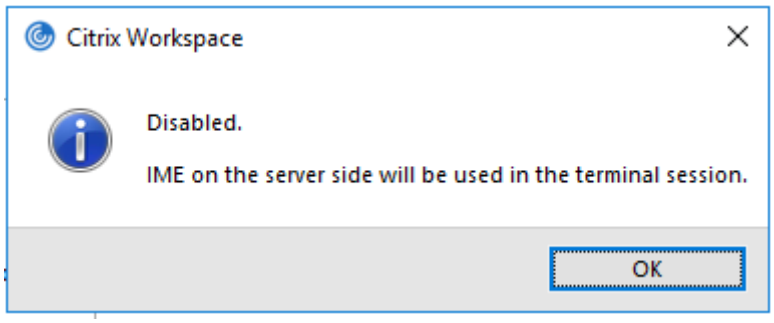
> **Nota:**
>
> Si utiliza un sistema operativo Windows 10, versión 2004, es posible que tenga problemas técnicos al usar la función IME en una sesión. Esos problemas son el resultado de una limitación de terceros. Para obtener más información, consulte el artículo de asistencia de Microsoft.

**Configurar el IME de cliente genérico mediante la interfaz de línea de comandos:**

- Para habilitar el IME de cliente genérico, ejecute el comando `wfica32.exe /localime:on` desde la carpeta de instalación de la aplicación Citrix Workspace `C:\Program Files (x86)\Citrix\ICA Client`.



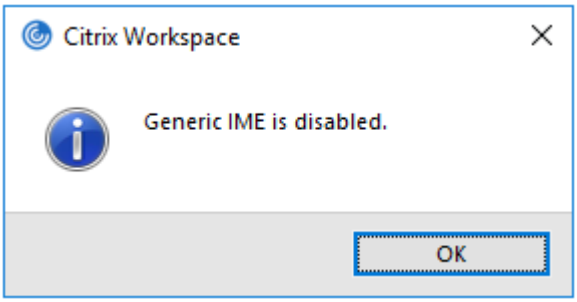

- Para inhabilitar el IME de cliente genérico, ejecute el comando `wfica32.exe /localime:off` desde la carpeta de instalación de la aplicación Citrix Workspace `C:\Program Files (x86)\Citrix\ICA Client`.



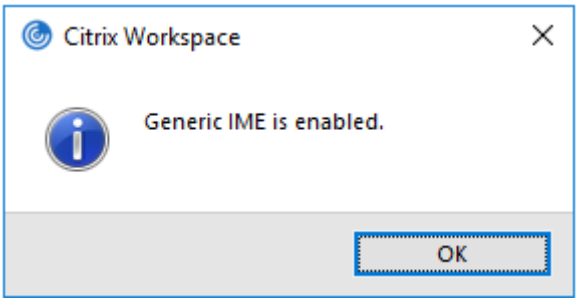

> **Nota:**
>
> Puede usar el modificador de línea de comandos `wfica32.exe /localime:on` para habilitar tanto el IME de cliente genérico como la sincronización de la distribución de teclado.

- Para inhabilitar el IME de cliente genérico, ejecute el comando `wfica32.exe /localgenericime:off` desde la carpeta de instalación de la aplicación Citrix Workspace `C:\Program Files (x86)\Citrix\ICA Client`. Este comando no afecta a los parámetros de sincronización de distribución de teclado.




Si ha inhabilitado el IME de cliente genérico desde la interfaz de línea de comandos, puede habilitar la función de nuevo mediante el comando `wfica32.exe /localgenericime:on`.




**Activar/desactivar:**

La aplicación Citrix Workspace admite la activación o desactivación de esta función. Ejecute `wfica32.exe /localgenericime:on` para habilitarla o inhabilitarla. Sin embargo, los parámetros de sincronización de distribución de teclado tienen prioridad sobre este comando conmutador. Si la sincronización de la distribución de teclado está **desactivada**, la activación con el conmutador no habilita el IME de cliente genérico.

**Configurar el IME de cliente genérico mediante la interfaz gráfica de usuario:**

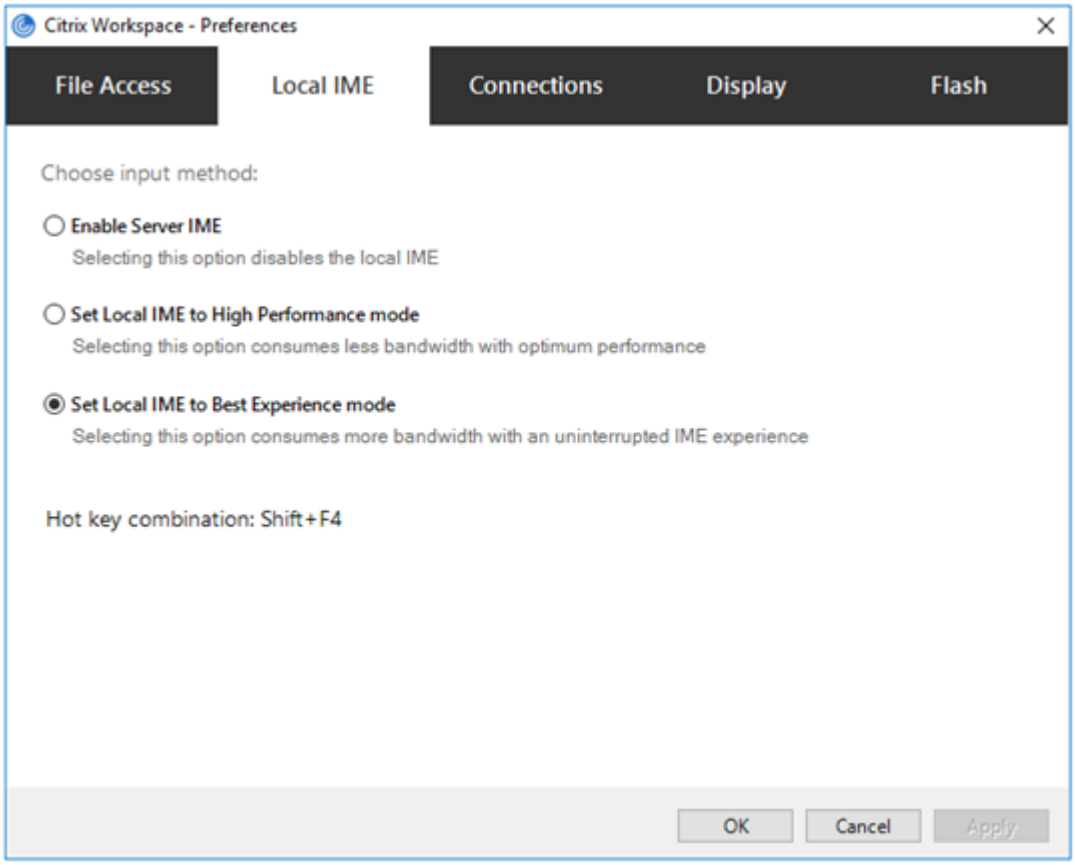
El IME de cliente genérico requiere el VDA 7.13 o una versión más reciente.

La función de IME de cliente genérico se puede habilitar mediante la habilitación de la sincronización de la distribución de teclado. Para obtener más información, consulte Sincronizar la distribución del teclado.

La aplicación Citrix Workspace permite configurar diferentes opciones para usar el IME de cliente genérico. Se puede seleccionar alguna de estas opciones en función de los requisitos y el uso.

1. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace en el área de notificaciones y seleccione **Central de conexiones**.
2. Seleccione **Preferencias** y haga clic en **IME local**.




Las siguientes opciones están disponibles para los distintos modos de IME:

1. **Habilitar IME del servidor:** Inhabilita el IME local y solo se pueden utilizar los idiomas establecidos en el servidor.
2. **Definir IME local en modo de alto rendimiento:** Usa el IME local con ancho de banda limitado. Esta opción restringe la funcionalidad de la ventana de candidatos.
3. **Definir IME local en modo de experiencia óptima:** Usa el IME local con la mejor experiencia de usuario. Esta opción consume mucho ancho de banda. De forma predeterminada, se selecciona esta opción cuando se habilita el IME de cliente genérico.

Los cambios solo se aplican a la sesión actual.

**Habilitar la configuración de teclas de acceso rápido mediante un editor del Registro:**

Cuando el IME de cliente genérico está habilitado, se puede usar **MAYÚS + F4** para seleccionar distintos modos de IME. Las diferentes opciones de modos IME aparecen en la esquina superior derecha de la sesión.

De forma predeterminada, la tecla de acceso rápido para el IME de cliente genérico está inhabilitada.

En el Editor del Registro, vaya a `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Key`.

Seleccione **AllowHotKey** y cambie el valor predeterminado a 1.

Puede utilizar las teclas de acceso rápido **Mayús+F4** para seleccionar diferentes modos de IME en las sesiones.

Las diferentes opciones de los modos de IME aparecen en la esquina superior derecha de la sesión al usar este atajo.


**Limitaciones:**

- El IME de cliente genérico no admite las aplicaciones UWP (Universal Windows Platform) tales como IU de búsqueda y el explorador Edge del sistema operativo Windows 10. Como solución temporal, use el editor IME del servidor en su lugar.
- El editor IME genérico del cliente no es compatible con Internet Explorer 11 en **modo protegido**. Como solución temporal, puede inhabilitar el modo protegido en las **Opciones de Internet**. Para inhabilitarlo, haga clic en **Seguridad** y desmarque la casilla **Habilitar modo protegido**.

### Codificación de vídeo H.265

La aplicación Citrix Workspace admite el uso del códec de vídeo H.265 para la aceleración de hardware de vídeos y gráficos remotos. Es necesario que se admita el códec de vídeo H.265 y que esté habilitado tanto en el VDA como en la aplicación Citrix Workspace. Si la GPU del dispositivo de punto final no admite la decodificación H.265 mediante la interfaz DXVA, la configuración de directiva "Decodificación H265 para gráficos" se ignora y la sesión recurre al códec de vídeo H.264.

**Requisitos previos:**

1. VDA 7.16 y versiones posteriores.
2. Habilite la directiva **Optimizar para cargas de trabajo de gráficos 3D** en el VDA.
3. Habilite la directiva **Usar codificación por hardware para códec de vídeo** en el VDA.

> **Nota:**
>
> La codificación H.265 solo se admite en las GPU de NVIDIA.

Esta función está **Inhabilitada** de forma predeterminada en la aplicación Citrix Workspace para Windows.

**Configurar la aplicación Citrix Workspace para usar la codificación de vídeo H.265 mediante la plantilla administrativa de GPO de Citrix:**

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Citrix Workspace** > **Experiencia de usuario**.
3. Seleccione la directiva **Decodificación H265 para gráficos**.
4. Seleccione **Enabled**.
5. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**

**Configurar la codificación de vídeo H.265 mediante el Editor del Registro:**

**Habilitar la codificación de vídeo H.265 en una red no unida a un dominio en un sistema operativo de 32 bits:**

1. Abra el Editor del Registro mediante regedit en el comando Ejecutar.
2. Vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Graphics Engine`.
3. Cree una clave DWORD con el nombre **EnableH265** y establezca el valor de la clave en 1.

**Habilitar la codificación de vídeo H.265 en una red no unida a un dominio en un sistema operativo de 64 bits:**

1. Abra el Editor del Registro mediante regedit en el comando Ejecutar.
2. Vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\ICA Client\Graphics Engine`.
3. Cree una clave DWORD con el nombre EnableH265 y establezca el valor de la clave en 1.

Vuelva a iniciar la sesión para que los cambios surtan efecto.

> **Nota:**
>
> - Si la directiva **Aceleración de hardware para gráficos** está inhabilitada en la plantilla administrativa de GPO de la aplicación Citrix Workspace para Windows, la configuración de directiva **Decodificación H265 para gráficos** se ignora y esta función no funciona.
> - Ejecute la herramienta HDX Monitor 3.x para saber si el codificador de vídeo H.265 está habilitado dentro de las sesiones. Para obtener más información acerca de la herramienta HDX Monitor 3.x, consulte el artículo CTX135817 de Knowledge Center.

## Barra de idioma y distribución del teclado

### Distribución del teclado

> **Nota:**
>
> Puede ocultar total o parcialmente las opciones de la hoja de Preferencias avanzadas, disponible en el icono de la aplicación Citrix Workspace del área de notificaciones. Para obtener más información, consulte Hoja de Preferencias avanzadas.

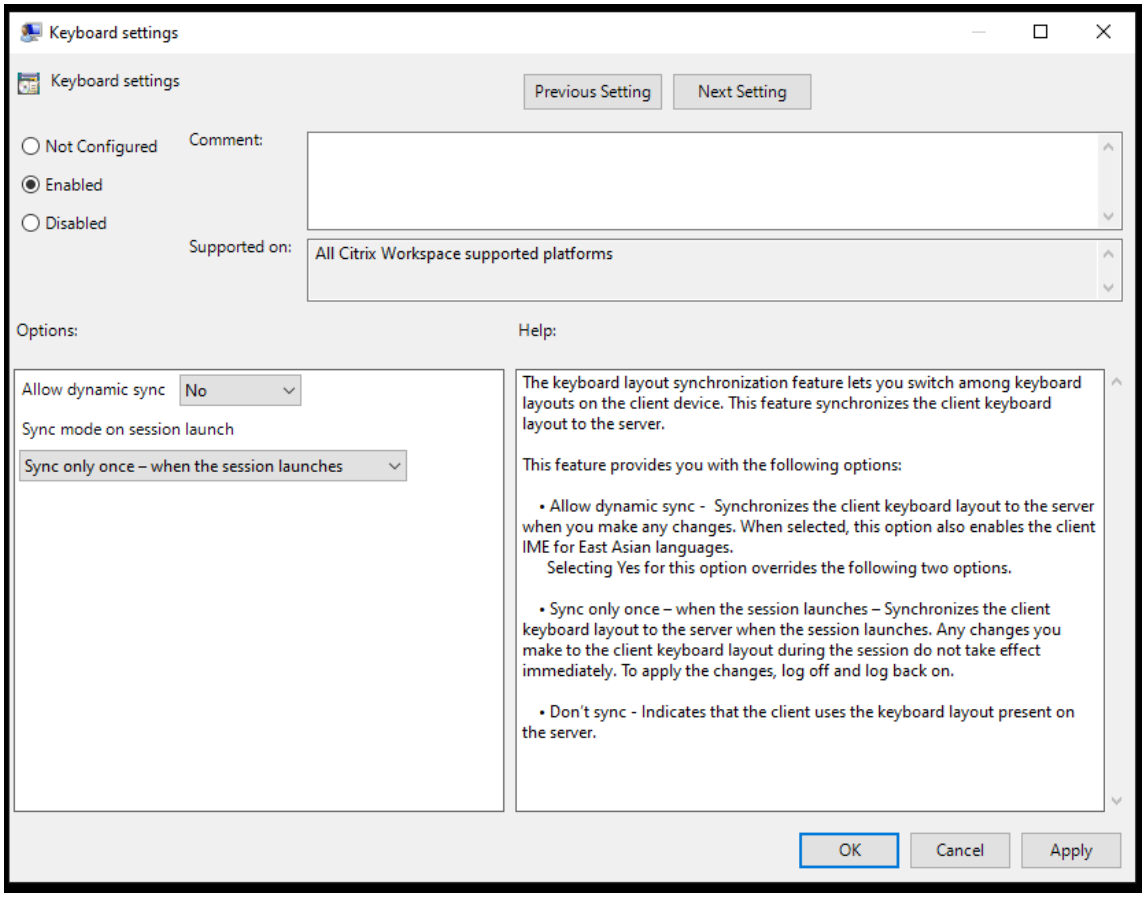
La sincronización de la distribución del teclado le permite cambiar entre distintas distribuciones de teclado preferidas en el dispositivo cliente. Esta función está inhabilitada de forma predeterminada. La sincronización de la distribución del teclado permite que la distribución del teclado del cliente se sincronice automáticamente con la sesión de aplicaciones y escritorios virtuales.

**Para configurar la sincronización de la distribución del teclado mediante la plantilla administrativa de GPO:**

> **Nota:**
>
> La configuración de GPO tiene prioridad sobre las configuraciones de StoreFront y de la GUI.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En los nodos **Configuración del equipo** o **Configuración del usuario**, vaya a **Plantillas administrativas** > **Plantillas administrativas clásicas (ADM)** > **Componentes de Citrix** > **Citrix Workspace** > **Experiencia de usuario**.
3. Seleccione la directiva **Parámetros del teclado**.




4. **Habilítela** y seleccione una de estas opciones:
   - **Permitir sincronización dinámica**: En el menú desplegable, seleccione **Sí** o **No**. Esta opción sincroniza la distribución del teclado del cliente con el servidor al cambiar la distribución del teclado del cliente. Al seleccionar esta opción, también se habilita el editor IME del cliente para idiomas de Asia Oriental.
     Al seleccionar **Sí** para esta opción, se anulan las dos opciones siguientes.
   - **Modo de sincronización al iniciar la sesión**: En el menú desplegable, seleccione una de estas opciones:
     - **Sincronizar solo una vez: cuando se inicia la sesión**: Sincroniza la distribución del teclado del cliente con la del servidor cuando se inicia la sesión. Los cambios que haga en la distribución del teclado del cliente durante la sesión no surtirán efecto inmediatamente. Para aplicar los cambios, cierre la sesión y vuelva a iniciarla.
     - **No sincronizar**: Indica que el cliente utiliza la distribución del teclado presente en el servidor.
5. Seleccione **Aplicar** y **Aceptar**.

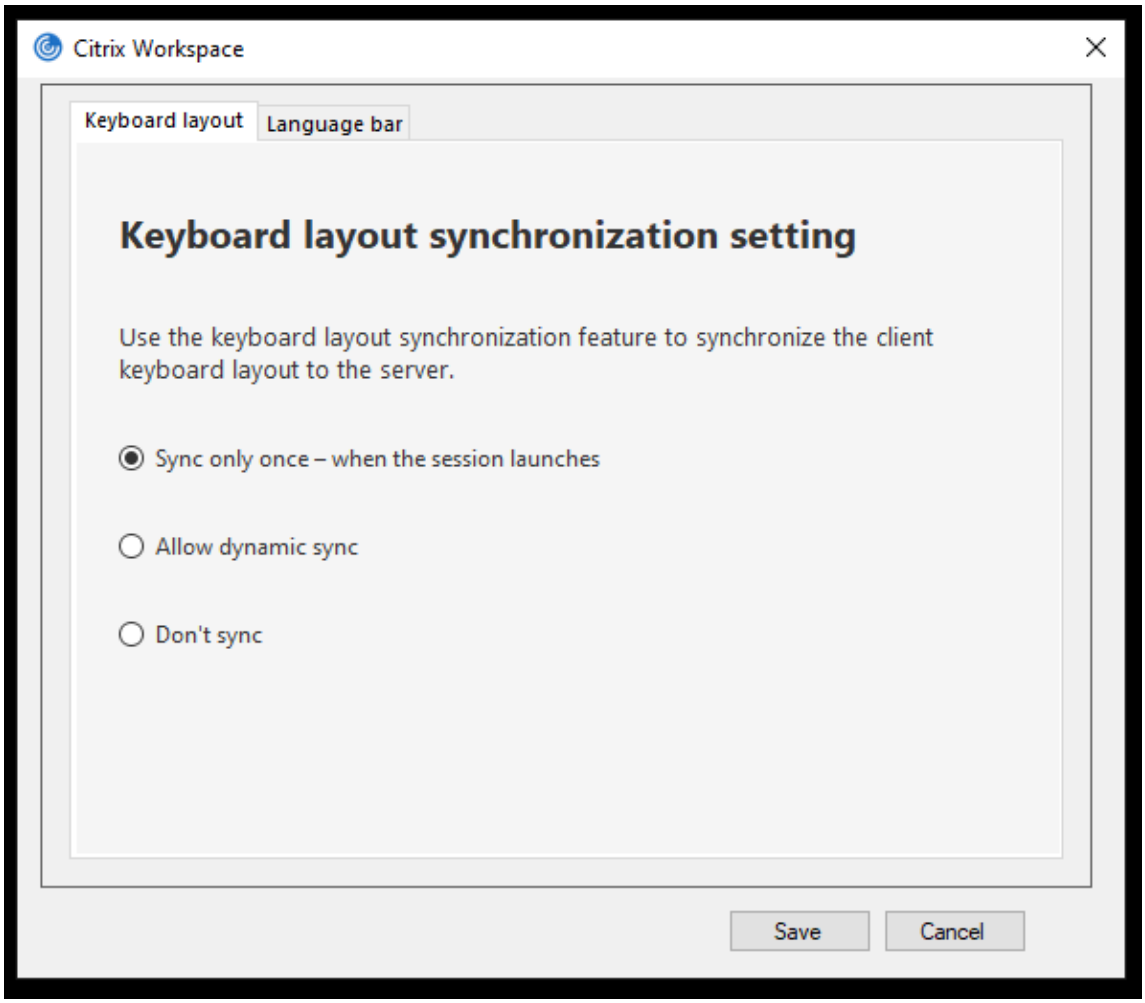
**Para configurar la sincronización de la distribución del teclado mediante la interfaz gráfica de usuario:**

1. Desde el icono de la aplicación Citrix Workspace del área de notificaciones, seleccione **Prefer-**

**encias avanzadas** > **Barra de idioma y teclado**.

Aparecerá el cuadro de diálogo **Barra de idioma y teclado**.




2. Seleccione una de estas opciones:
   - **Sincronizar solo una vez: cuando se inicia la sesión**: Indica que la distribución del teclado se sincroniza desde el VDA solo una vez al iniciarse la sesión.
   - **Permitir sincronización dinámica**: Indica que la distribución del teclado se sincroniza de manera dinámica con el VDA al cambiar el teclado del cliente en una sesión.
   - **No sincronizar**: Indica que el cliente utiliza la distribución del teclado presente en el servidor.
3. Haga clic en **Guardar**.

**Para configurar la sincronización de la distribución del teclado mediante la interfaz de línea de comandos:**

Ejecute este comando desde la carpeta de instalación de la aplicación Citrix Workspace para Windows.

Normalmente, la carpeta de instalación de la aplicación Citrix Workspace se encuentra en `C:\Program files (x86)\Citrix\ICA Client`.

- Para habilitarla: `wfica32:exe /localime:on`
- Para inhabilitarla: `wfica32:exe /localime:off`

La opción de distribución de teclado del cliente activa el editor IME (Input Method Editor) del cliente. Si los usuarios que trabajan en japonés, chino o coreano prefieren usar el editor IME del servidor, deben inhabilitar la opción de distribución del teclado del cliente. Para ello, deben seleccionar **No** o ejecutar `wfica32:exe /localime:off`. La sesión recurrirá a la distribución de teclado que suministre el servidor remoto cuando se conecten a la sesión siguiente.

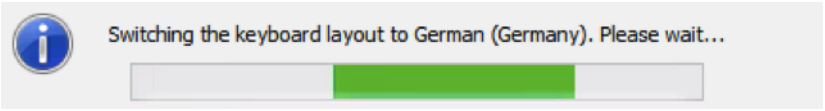
En ocasiones, el cambio a la distribución de teclado del cliente no tiene efecto en una sesión activa. Para resolver este problema, cierre la sesión en la aplicación Citrix Workspace y vuelva a iniciarla.

#### Configurar la sincronización del teclado en Windows VDA

> **Nota:**
>
> Este procedimiento solo se aplica a Windows Server 2016 y versiones posteriores. En Windows Server 2012 R2 y versiones anteriores, la función de sincronización del teclado está habilitada de forma predeterminada.

1. Abra el Editor del Registro y vaya a `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Cree la entrada DWORD `DisableKeyboardSync` y establezca su valor en `0`.
   `1` inhabilita la función de sincronización de distribución del teclado.
3. Vuelva a iniciar la sesión para que los cambios surtan efecto.

Una vez habilitada la distribución del teclado tanto en el VDA como en la aplicación Citrix Workspace, aparece esta ventana al cambiar de distribución del teclado.




Esta ventana indica que la distribución del teclado de la sesión se va a cambiar a la distribución del teclado del cliente.

#### Configurar la sincronización del teclado en Linux VDA

Inicie el símbolo del sistema y ejecute este comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\CurrentControlSet
\Control\Citrix\LanguageBar"-v "SyncKeyboardLayout"-d "0x00000001"
```

Reinicie el VDA para que los cambios surtan efecto.

Para obtener más información sobre la función de sincronización de distribución del teclado en Linux VDA, consulte Sincronización de la distribución de teclado dinámico.

**Ocultar el diálogo de notificación del cambio de distribución del teclado:**

El diálogo de notificación de cambio de distribución del teclado permite saber si la sesión VDA cambia la distribución del teclado. Para que el cambio de distribución del teclado se efectúe, se necesitan aproximadamente dos segundos. Tras ocultar el cuadro de diálogo de notificación, espere un tiempo antes de comenzar a escribir para evitar la introducción de caracteres incorrectos.

> **Advertencia**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

**Ocultar el diálogo de notificación del cambio de distribución del teclado mediante el Editor del Registro:**

1. Abra el Editor del Registro y vaya a `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Cree una clave de valor de cadena con el nombre **HideNotificationWindow**.
3. Establezca DWORD con el valor **1**.
4. Haga clic en **Aceptar**.
5. Vuelva a iniciar la sesión para que los cambios surtan efecto.

**Limitaciones:**

- Las aplicaciones remotas que se ejecutan con privilegios elevados (por ejemplo, hacer clic con el botón secundario en el icono de una aplicación y elegir la opción “Ejecutar como administrador”) no se pueden sincronizar con la distribución de teclado del cliente. Como solución temporal, cambie manualmente la distribución del teclado en el lado del servidor (VDA) o inhabilite el Control de cuentas de usuario (UAC).
- Si el usuario cambia la distribución del teclado en el cliente por una distribución que no es compatible en el servidor, la función de sincronización de la distribución del teclado se inhabilita por motivos de seguridad. Una distribución de teclado no reconocida se considera una amenaza potencial para la seguridad. Para restaurar la función de la sincronización de distribución del teclado, cierre la sesión y vuelva a iniciarla.
- En una sesión RDP, no se puede cambiar la distribución del teclado con los accesos directos Alt + Mayús. Como solución temporal, use la barra de idioma en la sesión RDP para cambiar la distribución del teclado.

**Barra de idioma**

La barra de idioma muestra el idioma de entrada preferido en una sesión. La barra de idioma aparece en una sesión de forma predeterminada.

> **Nota:**
>
> Esta función está disponible en sesiones con VDA 7.17 y versiones posteriores.

**Configurar la barra de idioma mediante la plantilla administrativa de GPO:**

La barra de idioma muestra el idioma de entrada preferido en una sesión de aplicación.

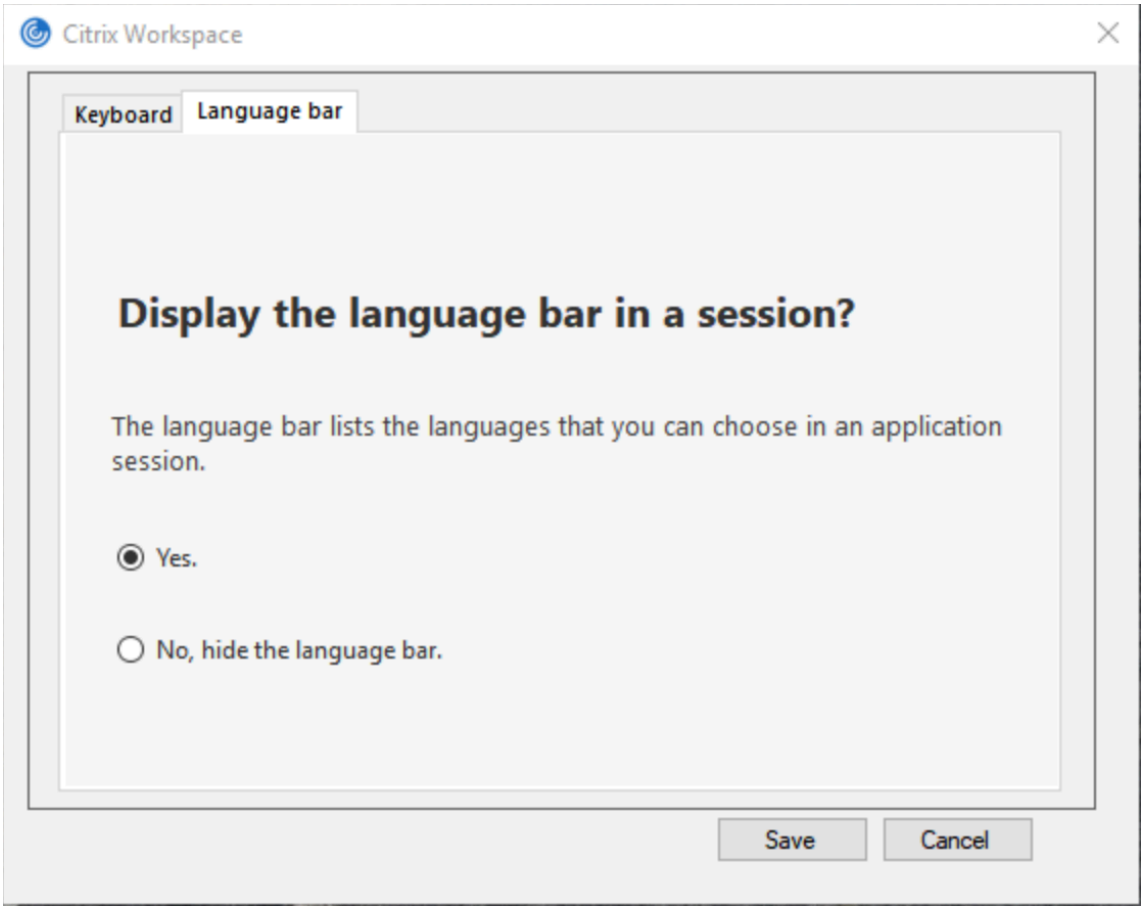
1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En los nodos **Configuración del equipo** o **Configuración del usuario**, vaya a **Plantillas administrativas** > **Plantillas administrativas clásicas (ADM)** > **Componentes de Citrix** > **Citrix Workspace** > **Experiencia de usuario**.
3. Seleccione la directiva **Barra de idioma**.
4. **Habilítela** y seleccione una de estas opciones:
   - Sí: Indica que la barra de idioma se muestra en la sesión de una aplicación.
   - No, ocultar la barra de idioma: Indica que la barra de idioma se oculta en la sesión de una aplicación.
5. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**

**Configurar la barra de idioma mediante la interfaz gráfica de usuario:**

1. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace en el área de notificaciones y seleccione **Preferencias avanzadas**.
2. Seleccione **Barra de idioma y teclado**.
3. Seleccione la ficha **Barra de idioma**.
4. Seleccione una de estas opciones:
   a) Sí: La barra de idioma se muestra en una sesión.
   b) No; ocultar la barra de idioma: La barra de idioma se oculta en una sesión.
5. Haga clic en **Guardar**.

   Los cambios de configuración surten efecto de inmediato.




> **Nota:**
>
> - Puede cambiar la configuración en una sesión activa.
> - La barra de idioma remota no aparece en una sesión si solo hay un idioma de entrada.

**Ocultar la barra de idioma en la hoja de Preferencias avanzadas:**

Puede utilizar el Registro para ocultar la ficha de la barra de idioma a fin de que esta no aparezca en la hoja **Preferencias avanzadas**.

1. Abra el Editor del Registro.
2. Vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\LocalIME`.
3. Cree una clave de valor DWORD, **ToggleOffLanguageBarFeature**, y establézcala en **1** para ocultar la opción de barra de idioma en la hoja “Preferencias avanzadas”.

### Compatibilidad con USB

Si se admite USB, se permite interactuar con una amplia variedad de dispositivos USB en una conexión a Citrix Virtual Apps and Desktops y Citrix DaaS. Puede conectar dispositivos USB a sus equipos y esos dispositivos se pueden usar de manera remota en el escritorio virtual. Los dispositivos

USB disponibles para la comunicación remota son, entre otros, las unidades flash, los teléfonos inteligentes, las impresoras, los escáneres, los reproductores MP3, los dispositivos de seguridad y las PC tabletas. Mediante una preferencia de la barra de herramientas, los usuarios de Desktop Viewer pueden controlar si los dispositivos USB se encuentran disponibles en aplicaciones y escritorios de Citrix Virtual Apps and Desktops y Citrix DaaS.

Las funciones isócronas de los dispositivos USB (como cámaras web, micrófonos, altavoces y auriculares) se admiten en entornos LAN típicos de baja latencia o alta velocidad. Este entorno permite que estos dispositivos interactúen con paquetes, como Microsoft Office Communicator y Skype.

Los siguientes tipos de dispositivos se admiten directamente en una sesión de aplicaciones y escritorios virtuales, y por lo tanto no ofrecen la funcionalidad USB:

- Teclados
- Mouse
- Tarjetas inteligentes

Los dispositivos USB especializados (por ejemplo, los teclados Bloomberg y mouse 3D) pueden configurarse para utilizar la funcionalidad USB. Para obtener información sobre cómo configurar los teclados Bloomberg, consulte Configurar teclados Bloomberg.

Para obtener información sobre cómo configurar reglas de directivas para otros dispositivos USB especializados, consulte el artículo CTX122615 en Knowledge Center.

De manera predeterminada, existen ciertos tipos de dispositivos USB que no se admiten para la comunicación remota a través de Citrix Virtual Apps and Desktops y Citrix DaaS. Por ejemplo, un usuario puede tener una tarjeta de interfaz de red conectada a la placa del sistema mediante un dispositivo USB interno. Colocar este dispositivo en comunicación remota no sería apropiado. Los siguientes tipos de dispositivos USB no se admiten de forma predeterminada en sesiones de aplicaciones y escritorios virtuales:

- Dispositivos Bluetooth
- Tarjeta NIC integrada
- Hubs USB
- Adaptadores gráficos USB

Los dispositivos USB conectados a un concentrador se pueden conectar remotamente pero no se puede conectar el concentrador propiamente dicho.

Los siguientes tipos de dispositivos USB no se admiten de forma predeterminada en sesiones de aplicaciones virtuales:

- Dispositivos Bluetooth
- Tarjeta NIC integrada
- Hubs USB
- Adaptadores gráficos USB

- Dispositivos de sonido
- Dispositivos de almacenamiento masivo

**Funcionamiento de la compatibilidad con USB:**

Cuando un usuario conecta un dispositivo USB, éste se comprueba con la directiva USB y, si se lo admite, se lo coloca en comunicación remota con el escritorio virtual. Si la directiva predeterminada rechaza un dispositivo, solo estará disponible para el escritorio local.

Cuando un usuario conecta un dispositivo USB, se muestra una notificación para informar al usuario sobre el nuevo dispositivo. El usuario puede seleccionar qué dispositivos USB deben conectarse de forma remota al escritorio virtual cada vez que se conectan. También, el usuario puede configurar la compatibilidad con USB para que todos los dispositivos USB que se conecten antes o durante una sesión se comuniquen automáticamente de forma remota con el escritorio virtual que esté en primer plano.

#### Clases de dispositivos USB que se admiten de manera predeterminada

Las reglas de directivas USB predeterminadas permiten diferentes clases de dispositivos USB.

A pesar de incluirse en esta lista, algunas clases están solo disponibles de forma remota en las sesiones de aplicaciones y escritorios virtuales después de una configuración adicional. Dichas clases de dispositivos USB son las siguientes.

- **Audio (clase 01):** Incluye los dispositivos de entrada de audio (micrófonos), los dispositivos de salida de audio y los controladores MIDI. Los dispositivos de audio modernos suelen utilizar transferencias isócronas compatibles con XenDesktop 4 y versiones posteriores. El audio (clase 01) no es aplicable a las aplicaciones virtuales, ya que estos dispositivos no están disponibles para la comunicación remota en aplicaciones virtuales mediante la funcionalidad USB.

> **Nota:**
>
> Algunos dispositivos específicos (por ejemplo, teléfonos VOIP) requieren una configuración adicional. Para obtener más información, consulte el artículo CTX123015 de Knowledge Center.

- **Dispositivos de interfaz física (clase 05):** Estos dispositivos son similares a los dispositivos de interfaz de usuario (HID) pero, en general, proporcionan respuesta o información en "tiempo real". Pueden ser joysticks con fuerza de respuesta, plataformas de movimiento y exoesqueletos con fuerza de respuesta.
- **Digitalización de imágenes fijas (clase 06):** Escáneres y cámaras digitales. Las cámaras digitales suelen admitir la clase de digitalización de imagen fija que utiliza el protocolo de transferencia de imágenes (PTP) o el protocolo de transferencia multimedia (MTP) para transferir imágenes a un equipo u otro dispositivo periférico. Las cámaras también pueden aparecer como dispositivos de almacenamiento masivo. Es posible configurar una cámara para que utilice cualquiera de las clases desde los menús de configuración que proporciona la propia cámara.

> **Nota:**
>
> Si una cámara aparece como un dispositivo de almacenamiento masivo, se utiliza la asignación de unidades del cliente y no se necesita la funcionalidad USB.

- **Impresoras (clase 07):** En general, la mayoría de las impresoras se incluyen en esta clase, aunque algunas utilizan protocolos específicos del fabricante (clase ff). Las impresoras multifunción pueden tener un concentrador interno o ser dispositivos compuestos. En ambos casos, el elemento de impresión generalmente utiliza la clase de la impresora y el elemento de fax o de escaneado utiliza otra clase, por ejemplo, la digitalización de imágenes fijas.

  Las impresoras normalmente funcionan de forma adecuada sin la funcionalidad USB.

  > **Nota**
  >
  > Esta clase de dispositivo (en particular, impresoras con funciones de escaneado) requiere configuración adicional. Para obtener instrucciones, consulte el artículo CTX123015 de Knowledge Center.

- **Almacenamiento masivo (clase 08):** Los dispositivos de almacenamiento masivo más comunes son las unidades flash USB. Otros son las unidades de disco duro con conexión USB, las unidades de CD/DVD y los lectores de tarjetas SD/MMC. Existe una amplia variedad de dispositivos con almacenamiento interno que también presentan una interfaz de almacenamiento masivo y que incluyen los reproductores multimedia, las cámaras digitales y los teléfonos celulares. El almacenamiento masivo (clase 08) no es aplicable a las aplicaciones virtuales, ya que estos dispositivos no están disponibles para la comunicación remota en aplicaciones virtuales mediante la funcionalidad USB. Las subclases conocidas, entre otras, son:

  - 01 Dispositivos flash limitados
  - 02 Dispositivos CD/DVD típicos (ATAPI/MMC-2)
  - 03 Dispositivos de cinta típicos (QIC-157)
  - 04 Unidades de disquete típicas (UFI)
  - 05 Unidades de disquete típicas (SFF-8070i)
  - 06 La mayoría de los dispositivos de almacenamiento masivo utiliza esta variante de SCSI

  A menudo se puede acceder a los dispositivos de almacenamiento masivo a través de la asignación de unidades del cliente y por lo tanto no se requiere la funcionalidad USB.

- **Seguridad del contenido (clase 0d):** Los dispositivos para seguridad del contenido aplican la protección del contenido, generalmente para la administración de derechos digitales o para la gestión de licencias. Esta clase incluye las llaves.

- **Vídeo (clase 0e)**: La clase de vídeo abarca los dispositivos que se utilizan para manipular vídeo o material relacionado con vídeo. Dispositivos, como cámaras web, videograbadoras digitales, conversores de vídeo analógico, algunos sintonizadores de televisión y algunas cámaras digitales que admiten la transmisión de video por streaming.

> **Importante**
>
> La mayoría de los dispositivos de transmisión de vídeo por streaming utilizan transferencias isócronas compatibles con XenDesktop 4 y versiones posteriores. Algunos dispositivos de vídeo (por ejemplo, cámaras web con detección de movimiento) requieren una configuración adicional. Para obtener instrucciones, consulte el artículo CTX123015 de Knowledge Center.

- **Atención médica personal (clase 0f):** Dispositivos de atención médica personal, como los sensores de presión arterial, los monitores de frecuencia cardíaca, podómetros, monitores de píldoras y espirómetros.
- **Específico del proveedor y de la aplicación (clases fe y ff):** Muchos dispositivos utilizan protocolos específicos del proveedor o protocolos no estandarizados por el consorcio USB, que generalmente se muestran como específicos del proveedor (clase ff).

#### Clases de dispositivos USB que se rechazan de manera predeterminada

Las reglas de directivas USB predeterminadas no permiten estas clases diferentes de dispositivos USB:

- Comunicaciones y control CDC (clases 02 y 0a). La directiva USB predeterminada no permite estos dispositivos porque es posible que uno de ellos proporcione la conexión al propio escritorio virtual.
- Dispositivos de interfaz humana (HID) (clase 03). Incluye una amplia variedad de dispositivos de entrada y de salida. Los dispositivos de interfaz humana (HID, por su sigla en inglés) típicos son los teclados, los mouse, los dispositivos señaladores, las tabletas gráficas, los controladores de juegos, los botones y las funciones de control.

  La subclase 01 se conoce como la clase de “interfaz de arranque” y se utiliza para los teclados y mouse.

  La directiva de USB predeterminada no permite teclados USB (clase 03, subclase 01, protocolo 1) ni mouse USB (clase 03, subclase 01, protocolo 2). Esto se debe a que la mayoría de los teclados y mouse se manejan adecuadamente sin el uso de USB. Además, suele ser necesario utilizar estos dispositivos de forma local y remota cuando se conecta a un escritorio virtual.
- Concentradores USB (clase 09). Los concentradores USB permiten conectar dispositivos adicionales al equipo local. No es necesario acceder a estos dispositivos de forma remota.
- Tarjeta inteligente (clase 0b). Los lectores de tarjeta inteligente abarcan los lectores de tarjeta inteligente con contacto y sin contacto, y los tokens USB con un chip inteligente incluido que equivale a la tarjeta.

  Se accede a los lectores de tarjeta inteligente mediante la comunicación remota de la tarjeta inteligente y no se necesita la funcionalidad USB.

- Controlador inalámbrico (clase e0). Es posible que algunos de estos dispositivos proporcionen acceso de red importante o conecten periféricos importantes, como mouse o teclados Bluetooth.

  La directiva USB predeterminada no permite estos dispositivos. No obstante, es posible que, en el caso de dispositivos particulares, sea apropiado proporcionar acceso al uso de USB.

- **Varios dispositivos de red (clase ef, subclase 04)**: Es posible que algunos de estos dispositivos ofrezcan un acceso peligroso a la red. La directiva USB predeterminada no permite estos dispositivos. No obstante, es posible que, en el caso de dispositivos particulares, sea apropiado proporcionar acceso al uso de USB.

#### Actualizar la lista de dispositivos USB disponibles para la comunicación remota

Modifique el archivo de plantilla de Citrix Workspace para Windows para actualizar el rango de dispositivos USB disponibles para la comunicación remota con los escritorios. Esta actualización le permite realizar cambios en Citrix Workspace para Windows mediante la directiva de grupo. El archivo se halla en esta carpeta de instalación:

`\C:\Program Files\Citrix\ICA Client\Configuration\en`

También puede modificar el Registro en cada dispositivo de usuario y agregar la siguiente clave de Registro:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB Type=String Name="DeviceRules" Value=

> **Importante**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Las reglas predeterminadas del producto se almacenan en:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB Tipo=MultiSz Nombre="DeviceRules" Valor=

No modifique las reglas predeterminadas del producto.

Para obtener más información acerca de la configuración de directivas de dispositivos USB, consulte Configuraciones de directiva de Dispositivos USB en la documentación de Citrix Virtual Apps and Desktops.

**Redirección de dispositivos USB compuestos**

USB 2.1 y versiones posteriores admiten la noción de dispositivos USB compuestos donde varios dispositivos secundarios comparten una única conexión con el mismo bus USB. Estos dispositivos emplean un solo espacio de configuración y una conexión de bus compartida, donde se utiliza un número de interfaz único 00-ff para identificar cada dispositivo secundario. Estos dispositivos no son lo mismo que un concentrador USB que proporciona un nuevo origen de bus USB para otros dispositivos USB con direcciones independientes para la conexión.

Los dispositivos compuestos encontrados en el dispositivo de punto final cliente se pueden reenviar al host virtual como una de estas dos opciones:

- Un solo dispositivo USB compuesto
- Un conjunto de dispositivos secundarios independientes (dispositivos divididos)

Cuando se reenvía un dispositivo USB compuesto, todo el dispositivo deja de estar disponible para el dispositivo de punto final. El reenvío también bloquea el uso local del dispositivo para todas las aplicaciones del dispositivo de punto final, incluido el cliente Citrix Workspace necesario para ofrecer una experiencia remota con HDX optimizado.

Considere un dispositivo con auriculares USB con dispositivo de audio y un botón HID para el control de volumen y silencio. Si todo el dispositivo se reenvía mediante un canal USB genérico, el dispositivo deja de estar disponible para la redirección por el canal de audio con HDX optimizado. Sin embargo, puede obtener una experiencia óptima cuando el audio se envía a través del canal de audio con HDX optimizado, a diferencia del audio enviado mediante controladores de audio del lado del host a través de la comunicación remota por USB genérico. Este comportamiento se produce porque los protocolos de audio USB suelen provocar ruido.

También nota problemas cuando el teclado del sistema o el dispositivo al que apunta forman parte de un dispositivo compuesto con otras funciones integradas necesarias para admitir sesiones remotas. Cuando se reenvía un dispositivo compuesto completo, el teclado o el mouse del sistema dejan de funcionar en el dispositivo de punto final, excepto en la sesión o la aplicación del escritorio remoto.

Para resolver estos problemas, Citrix recomienda dividir el dispositivo compuesto y reenviar solo las interfaces secundarias que usan un canal USB genérico. Este mecanismo garantiza que los demás dispositivos secundarios estén disponibles para su uso en las aplicaciones del dispositivo de punto final del cliente, incluida la aplicación Citrix Workspace que ofrece una experiencia con HDX optimizado, al tiempo que permite el reenvío y la disposición de los dispositivos necesarios a la sesión remota.

**Reglas de dispositivo:**

Al igual que los dispositivos USB normales, las reglas de dispositivo establecidas en la directiva o en la configuración de la aplicación Citrix Workspace del cliente en el dispositivo de punto final seleccionan los dispositivos compuestos para el reenvío. La aplicación Citrix Workspace usa estas reglas para decidir los dispositivos USB para los que permitir o impedir el reenvío a la sesión remota.

Cada regla consta de una palabra clave de acción (Permitir, Conectar o Denegar), dos puntos (**:**) y cero o más parámetros de filtro que coinciden con dispositivos reales en el subsistema USB de los dispositivos de punto final. Estos parámetros de filtro corresponden a los metadatos descriptores del dispositivo USB que utiliza cada dispositivo USB para identificarse.

Las reglas de dispositivo son texto no cifrado con cada regla en una sola línea y un comentario opcional precedido de un carácter **#**. Las reglas se cotejan de arriba a abajo (orden de prioridad descendente). Se aplica la primera regla que coincida con la interfaz del dispositivo o la interfaz secundaria. Se ignoran las reglas subsiguientes que seleccionen el mismo dispositivo o interfaz.

Reglas de dispositivo de ejemplo:

- ALLOW: vid=046D pid=0102 # Permite un dispositivo específico por vid/pid
- ALLOW: vid=0505 class=03 subclass=01 # Permite cualquier pid para el proveedor 0505 cuando subclass=01
- DENY: vid=0850 pid=040C # Deniega un dispositivo específico (incluidos todos los dispositivos secundarios)
- DENY: class=03 subclass=01 prot=01 # Deniega todo dispositivo que coincida con todos los filtros
- CONNECT: vid=0911 pid=0C1C # Permite y se conecta automáticamente a un dispositivo específico
- ALLOW: vid=0286 pid=0101 split=01 # Divide este dispositivo y permite todas las interfaces
- ALLOW: vid=1050 pid=0407 split=01 intf=00,01 # Divide y permite solamente 2 interfaces
- CONNECT: vid=1050 pid=0407 split=01 intf=02 # Divide y se conecta automáticamente a la interfaz 2
- DENY: vid=1050 pid=0407 split=1 intf=03 # Evita que se conecte remotamente a la interfaz 03

Puede usar cualquiera de estos parámetros de filtro para aplicar reglas a los dispositivos detectados:

| Parámetro de filtro | Descripción |
|---|---|
| vid=xxxx | ID de proveedor del dispositivo USB (código hexadecimal de cuatro dígitos) |
| pid=xxxx | ID de producto del dispositivo USB (código hexadecimal de cuatro dígitos) |
| rel=xxxx | ID de versión del dispositivo USB (código hexadecimal de cuatro dígitos) |
| class=xx | Código de clase del dispositivo USB (código hexadecimal de dos dígitos) |
| subclass=xx | Código de subclase del dispositivo USB (código hexadecimal de dos dígitos) |

| Parámetro de filtro | Descripción |
|---|---|
| prot=xx | Código de protocolo del dispositivo USB (código hexadecimal de dos dígitos) |
| split=1 (o split=0) | Seleccione un dispositivo compuesto que dividir (o no dividir) |
| intf=xx[,xx,xx,…] | Seleccione un conjunto específico de interfaces secundarias de un dispositivo compuesto (lista separada por comas de códigos hexadecimales de dos dígitos) |

Los seis primeros parámetros seleccionan los dispositivos USB a los que se debe aplicar la regla. Si algún parámetro no se especifica, la regla coteja dispositivos con CUALQUIER valor para ese parámetro.

El foro de implementadores de USB mantiene una lista de valores definidos de clase, subclase y protocolo en Defined Class Codes. USB-IF también conserva una lista de los ID de proveedores registrados. Puede comprobar los ID de proveedor, producto, versión e interfaz de un dispositivo específico directamente en el administrador de dispositivos de Windows o con una herramienta gratuita como UsbTreeView.

Cuando están presentes, los dos últimos parámetros solo se aplican a dispositivos USB compuestos. El parámetro de división determina si un dispositivo compuesto debe reenviarse como dispositivos divididos o como un solo dispositivo compuesto.

- *Split=1* indica que las interfaces secundarias seleccionadas de un dispositivo compuesto deben reenviarse como dispositivos divididos.
- *Split=0* indica que el dispositivo compuesto no se debe dividir.

> **Nota:**
>
> Si el parámetro de división se omite, se presupone que *Split=0*.

El parámetro *intf* selecciona las interfaces secundarias específicas del dispositivo compuesto al que debe aplicarse la acción. Si se omite, la acción se aplica a todas las interfaces del dispositivo compuesto.

Considere un dispositivo compuesto de auriculares USB con tres interfaces:

- Interfaz 0: Dispositivos de punto final de clase audio
- Interfaz 3: Dispositivos de punto final de clase HID (botones de volumen y silencio)
- Interfaz 5: Interfaz de administración/actualización

Las reglas sugeridas para este tipo de dispositivo son:

- CONNECT: vid=047F pid=C039 split=1 intf=03 # Permite y se conecta automáticamente a un dispositivo HID
- DENY: vid=047F pid=C039 split=1 intf=00 # Deniega dispositivos de punto final de audio
- ALLOW: vid=047F pid=C039 split=1 intf=05 # Permite la interfaz de administración, pero no se conecta automáticamente

**Habilitar la directiva de reglas de dispositivo:**

La aplicación Citrix Workspace para Windows incluye un conjunto de reglas de dispositivo predeterminadas que filtra ciertas clases no deseadas de dispositivos y permiten aquellas que los clientes suelen encontrar.

Puede comprobar estas reglas de dispositivo predeterminadas en el Registro del sistema en uno de estos dos lugares:

- `HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\GenericUSB` (Windows de 32 bits)
- `HKEY_LOCAL_MACHINE\Software\WOW6432Node\Citrix\ICA Client\GenericUSB` (Windows de 64 bits), en el valor de multicadena **DeviceRules**.

Sin embargo, en la aplicación Citrix Workspace para Windows, puede aplicar la directiva **Reglas de dispositivos USB** para sobrescribir estas reglas predeterminadas.

Para habilitar la directiva de reglas de dispositivo para la aplicación Citrix Workspace para Windows:

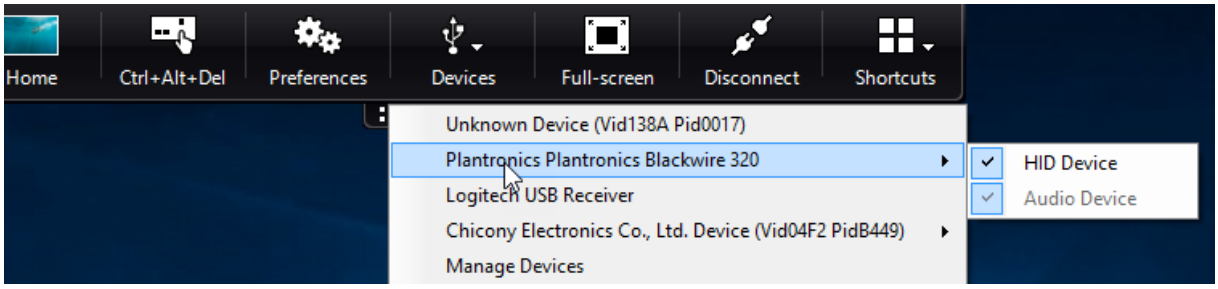
1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del usuario**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Uso remoto de dispositivos cliente** > **Uso remoto de USB genérico**.
3. Seleccione la directiva **Reglas de dispositivos USB**.
4. Seleccione **Enabled**.
5. En el cuadro de texto **Reglas de dispositivos USB**, pegue (o modifique directamente) las reglas de dispositivos USB que se implementarán.
6. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**

Citrix recomienda conservar las reglas predeterminadas que se envían al cliente al crear esta directiva mediante la copia de las reglas originales y la inserción de reglas nuevas para modificar el comportamiento como se quiera.

**Conectar dispositivos USB:**

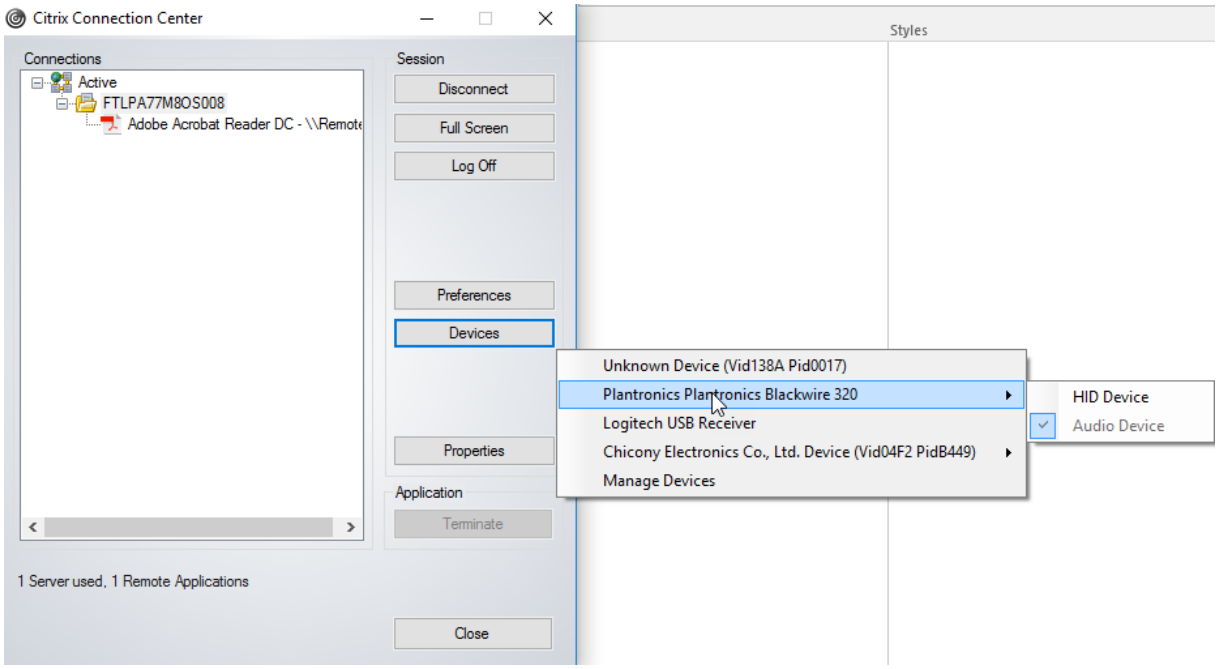
En una sesión de escritorio, los dispositivos USB divididos se muestran en Desktop Viewer, en **Dispositivos**. Además, los dispositivos USB divididos se pueden ver también en **Preferencias** > **Dispositivos**.




> **Nota:**
>
> La palabra clave CONNECT permite la conexión automática de un dispositivo USB. Sin embargo, si la palabra clave CONNECT no se utiliza al dividir un dispositivo USB compuesto para la redirección de USB genérico, debe seleccionar manualmente el dispositivo desde Desktop Viewer o la Central de conexiones para conectar un dispositivo permitido.

En una sesión de aplicación, los dispositivos USB divididos se muestran en la **Central de conexiones**.




**Para conectar automáticamente una interfaz:**

La palabra clave CONNECT introducida en la aplicación Citrix Workspace para Windows 2109 permite la redirección automática de dispositivos USB. La regla CONNECT puede reemplazar la regla ALLOW si el administrador permite que el dispositivo o determinadas interfaces se conecten automáticamente en la sesión.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del usuario**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Uso remoto de dispositivos cliente** > **Uso remoto de USB**

**genérico**.

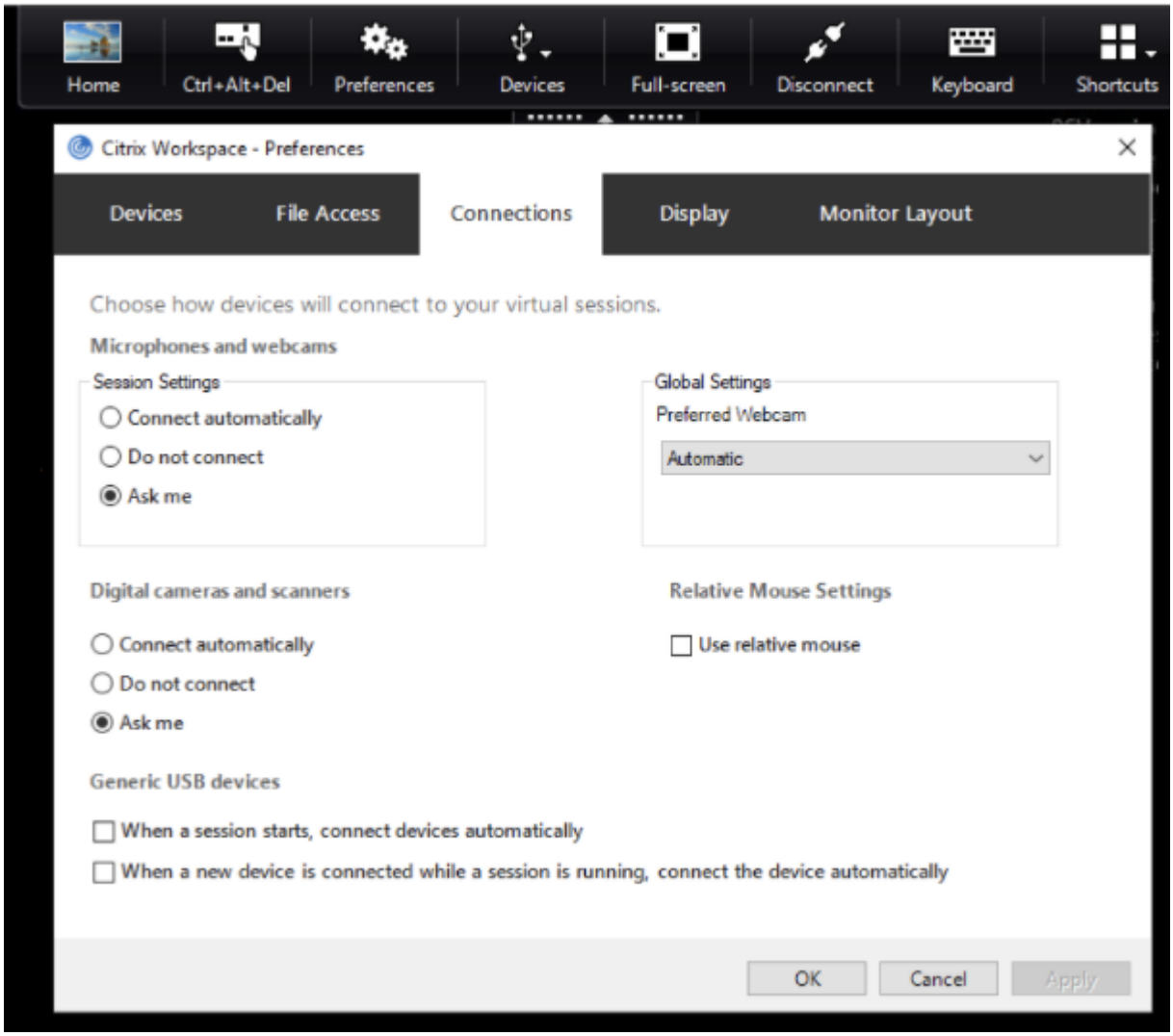
3. Seleccione la directiva **Reglas de dispositivos USB**.
4. Seleccione **Enabled**.
5. En el cuadro de texto **Reglas de dispositivos USB**, agregue el dispositivo USB que quiere que se conecte automáticamente.

   Por ejemplo: CONNECT: vid=047F pid=C039 split=01 intf=00,03 permite dividir un dispositivo compuesto, la conexión automática de las interfaces 00 y 03, y la restricción de otras interfaces de ese dispositivo.
6. Haga clic en **Aplicar** y **Aceptar** para guardar la directiva.

**Cambiar las preferencias de la conexión automática de los dispositivos USB:**

La aplicación Citrix Workspace conecta automáticamente dispositivos USB etiquetados con la acción CONNECT en función de las preferencias establecidas para el recurso de escritorio actual. Puede cambiar las preferencias en la barra de herramientas de **Desktop Viewer**, como se muestra en la siguiente imagen.




Las dos casillas situadas en la parte inferior del panel controlan si los dispositivos deben conectarse automáticamente o esperar conexiones manuales en la sesión. Estos parámetros no están habilitados de forma predeterminada. Puede cambiar las preferencias si los dispositivos USB genéricos deben conectarse automáticamente.

Si no, un administrador puede supeditar las preferencias de usuario mediante la implementación de las directivas correspondientes desde la plantilla administrativa de objetos de directiva de grupo de la aplicación Citrix Workspace. Las directivas de usuario y máquina se pueden encontrar en **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Uso remoto de dispositivos cliente** > **Uso remoto de USB genérico**. Las directivas correspondientes se etiquetan como Dispositivos USB existentes y Dispositivos USB nuevos, respectivamente.

**Cambiar la configuración predeterminada de dispositivos divididos:**

De forma predeterminada, la aplicación Citrix Workspace para Windows solo divide dispositivos compuestos que se etiquetan explícitamente como *Split=1* en las reglas de dispositivo. Sin embargo,

puede cambiar la disposición predeterminada para dividir todos los dispositivos compuestos que no están etiquetados con *Split=0* en una regla de dispositivo correspondiente.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del usuario**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Uso remoto de dispositivos cliente** > **Uso remoto de USB genérico**.
3. Seleccione la directiva **Dividir dispositivos**.
4. Seleccione **Enabled**.
5. Haga clic en **Aplicar** y **Aceptar** para guardar la directiva.

> **Nota:**
>
> Citrix recomienda usar reglas de dispositivo explícitas para identificar dispositivos o interfaces específicos que deben dividirse en lugar de cambiar el valor predeterminado. Esta configuración se retirará en una versión futura.

**Limitación:**

Citrix recomienda que no divida interfaces para una cámara web. Como solución alternativa, se puede redirigir el dispositivo a un dispositivo único mediante la redirección de USB genérico. Para obtener un mejor rendimiento, use el canal virtual optimizado.

#### Teclados Bloomberg

La aplicación Citrix Workspace admite el uso de teclados Bloomberg en una sesión de aplicaciones y escritorios virtuales. Los componentes necesarios se instalan con el plug-in. Puede activar la función de teclado Bloomberg durante la instalación de la aplicación Citrix Workspace para Windows o mediante el Editor del Registro.

Los teclados Bloomberg ofrecen otra funcionalidad en comparación con teclados estándar, lo que permite a los usuarios acceder a datos del mercado financiero y realizar transacciones bursátiles.

El teclado Bloomberg consta de varios dispositivos USB integrados en una shell física:

- El teclado
- Un lector de huellas dactilares
- Un dispositivo de audio
- Un concentrador USB para conectar todos estos dispositivos al sistema
- Botones HID, como, por ejemplo, Silenciar, Más volumen y Menos volumen, del dispositivo de audio

Además de la funcionalidad normal de estos dispositivos, el dispositivo de audio permite el uso de algunas teclas, el control del teclado y los LED del teclado.

Para usar la funcionalidad especializada dentro de una sesión, debe redirigir el dispositivo de audio como dispositivo USB. Esta redirección hace que el dispositivo de audio esté disponible para la sesión, pero impide que el dispositivo de audio se utilice localmente. Además, la funcionalidad especializada solo puede utilizarse con una sesión y no se puede compartir entre varias sesiones.

No se recomienda tener varias sesiones con teclados Bloomberg. El teclado solo funciona en entornos de sesión única.

**Para configurar teclados Bloomberg 5:**

Debe configurar varias interfaces del teclado Bloomberg. Desde la aplicación Citrix Workspace para Windows 2109, se presenta una nueva palabra clave CONNECT para permitir la conexión automática de dispositivos USB al iniciar las sesiones y al insertar dispositivos. La palabra clave CONNECT se puede usar para reemplazar la palabra clave ALLOW cuando el usuario quiera que una interfaz o un dispositivo USB se conecten automáticamente. En este ejemplo se utiliza la palabra clave CONNECT.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del usuario**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Uso remoto de dispositivos cliente** > **Uso remoto de USB genérico**.
3. Seleccione la directiva **Dividir dispositivos**.
4. Seleccione **Enabled**.
5. En el cuadro de texto **Reglas de dispositivos USB**, agregue estas reglas si no existen.
   - CONNECT: vid=1188 pid=A101 # Módulo biométrico de Bloomberg 5
   - DENY: vid=1188 pid=A001 split=01 intf=00 # Teclado principal Bloomberg 5
   - CONNECT: vid=1188 pid=A001 split=01 intf=01 # HID del teclado Bloomberg 5
   - DENY: vid=1188 pid=A301 split=01 intf=02 # Canal de audio del teclado Bloomberg 5
   - CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # HID del audio del teclado Bloomberg 5

   > **Nota:**
   >
   > Las líneas nuevas o el punto y coma se pueden utilizar para separar reglas, lo que permite leer valores del Registro de una línea o de varias líneas.
6. Haga clic en **Aplicar** y **Aceptar** para guardar la directiva.
7. En la ventana **Preferencias**, seleccione la ficha **Conexiones** y, a continuación, marque una o ambas casillas para conectar los dispositivos automáticamente. Se puede acceder a la ventana **Preferencias** desde la barra de herramientas del escritorio o desde el administrador de conexiones.

Este procedimiento deja el teclado Bloomberg 5 listo para su uso. Las reglas DENY mencionadas en los pasos aplican la redirección del teclado principal y del canal de audio a través de un canal optimizado,

pero no de USB genérico. Las reglas CONNECT permiten la redirección automática del módulo de huella digital, las teclas especiales en el teclado y las teclas relacionadas con el control de audio.

**Configurar teclados Bloomberg 4 o 3:**

> **Precaución**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

1. Busque la siguiente clave en el Registro:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`

2. Lleve a cabo una de las siguientes acciones:
   - Para habilitar esta función, configure una entrada de tipo DWORD y el nombre **EnableBloombergHID** con el valor 1.
   - Para inhabilitar esta función, establezca el valor en 0.

La funcionalidad para teclados Bloomberg 3 está disponible en el Online Plug-in 11.2 para Windows y versiones posteriores.

La funcionalidad para teclados Bloomberg 4 está disponible para Receiver para Windows 4.8 y versiones posteriores.

**Determinar si la funcionalidad para teclados Bloomberg está habilitada:**

- Para comprobar si la funcionalidad para teclados Bloomberg está habilitada en el Online Plug-in, compruebe los informes que genera Desktop Viewer sobre dispositivos de teclado Bloomberg. Si Desktop Viewer no se usa, puede comprobar el Registro en la máquina donde se ejecuta el Online Plug-in.
- Si la funcionalidad para teclados Bloomberg no está habilitada, Desktop Viewer muestra:
  - Dos dispositivos para el teclado Bloomberg 3, que aparece como **Bloomberg Fingerprint Scanner** y **Bloomberg Keyboard Audio**.
  - Un dispositivo redirigido por directiva para el teclado Bloomberg 4. Este dispositivo aparece como **Bloomberg LP Keyboard 2013**.
- Si la funcionalidad para teclados Bloomberg está habilitada, se muestran dos dispositivos en Desktop Viewer. Uno aparece como **Bloomberg Fingerprint Scanner** como antes y el otro como **Bloomberg Keyboard Features**.
- Si el controlador del dispositivo Bloomberg Fingerprint Scanner no está instalado, es posible que la entrada Bloomberg Fingerprint Scanner no aparezca en Desktop Viewer. Si falta la entrada, es posible que Bloomberg Fingerprint Scanner no esté disponible para la redirección. De

todos modos, puede comprobar el nombre del otro dispositivo Bloomberg donde está habilitada la funcionalidad para teclados Bloomberg.

- También puede comprobar el valor en el Registro para saber si la funcionalidad está habilitada: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB\EnableBloombergHID`

  Si el valor no existe o es 0 (cero), no se habilita la funcionalidad para teclados Bloomberg. Si el valor es 1, sí se habilita.

**Para habilitar el teclado Bloomberg:**

> **Nota:**
>
> Citrix Receiver para Windows 4.8 incorporó la compatibilidad con dispositivos compuestos a través de la directiva **Dividir dispositivos**. Sin embargo, para el teclado Bloomberg 4, debe usar la función de teclado Bloomberg en lugar de esta directiva.

La funcionalidad para teclados Bloomberg cambia el modo en que determinados dispositivos USB se redirigen a una sesión. Esta funcionalidad no está habilitada de forma predeterminada.

- Para habilitarla durante la instalación, especifique el valor de la propiedad **ENABLE_HID_REDIRECTION** en TRUE en la línea de comandos de instalación. Por ejemplo:

```
CitrixOnlinePluginFull.exe /silent
ADDLOCAL="ICA_CLIENT,PN_AGENT,SSON,USB"
ENABLE_SSON="no"INSTALLDIR="c:\test"
ENABLE_DYNAMIC_CLIENT_NAME="Yes"
DEFAULT_NDSCONTEXT="Context1,Context2"
SERVER_LOCATION="http://testserver.net"ENABLE_HID_REDIRECTION="TRUE"
```

- Para habilitarla después de instalar el Online Plug-in, modifique el Registro de Windows en el sistema donde se ejecuta el Online Plug-in:
  1. Abra el Editor del Registro.
  2. Vaya a esta clave: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`
  3. Si el valor **EnableBloombergHID** existe, modifíquelo para que los datos del valor sean 1.
  4. Si el valor **EnableBloombergHID** no existe, cree un valor DWORD con el nombre EnableBloombergHID e indique 1 como datos del valor.

**Inhabilitar la funcionalidad para el teclado Bloomberg:**

Puede inhabilitar la funcionalidad para teclados Bloomberg en el Online Plug-in de este modo:

1. Abra el Editor del Registro en el sistema donde se ejecuta el software de Online Plug-in.
2. Vaya a esta clave: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`

3. Si el valor **EnableBloombergHID** existe, modifíquelo para que los datos del valor sean 0 (cero).

   Si el valor **EnableBloombergHID** no existe, indica que la funcionalidad para teclados Bloomberg no está habilitada. En tal caso, no tiene que modificar ningún valor del Registro.

**Usar teclados Bloomberg sin habilitar la funcionalidad:**

- Puede usar el teclado sin habilitar la funcionalidad para teclados Bloomberg en el Online Plug-in. Sin embargo, no se puede beneficiar del uso compartido de la funcionalidad especializada en varias sesiones y es posible que disponga de un mayor ancho de banda de red para el audio.
- Las teclas normales del teclado Bloomberg están disponibles del mismo modo que cualquier otro teclado. No necesita tomar ninguna acción especial.
- Para usar las teclas Bloomberg especializadas, debe redirigir el dispositivo de audio del teclado Bloomberg a la sesión. Si utiliza Desktop Viewer, aparece el nombre del fabricante y el nombre del dispositivo de los dispositivos USB, y aparece **Bloomberg Keyboard Audio** para el dispositivo de audio del teclado Bloomberg.
- Para usar el lector de huellas digitales, debe redirigir el dispositivo a Bloomberg Fingerprint Scanner. Si los controladores del lector de huellas digitales no están instalados localmente, el dispositivo solo muestra una de estas opciones:
  - Si el Online Plug-in está configurado para conectar dispositivos automáticamente.
  - Permitir al usuario elegir si quiere conectar dispositivos.

  Además, si el teclado Bloomberg se conecta antes de establecer la sesión y los controladores del lector de huellas digitales no existen localmente, el lector de huellas digitales no aparece y no se puede usar en la sesión.

> **Nota:**
>
> Para Bloomberg 3, una sola sesión o el sistema local puede usar el lector de huellas dactilares y no se puede compartir. La redirección está prohibida en Bloomberg 4.

**Usar teclados Bloomberg después de habilitar la funcionalidad:**

- Si habilita la funcionalidad para teclados Bloomberg en el Online Plug-in, tiene la ventaja de compartir la funcionalidad especializada del teclado con varias sesiones. También dispone de menos ancho de banda de red para el audio.
- Habilitar la funcionalidad para teclados Bloomberg impide la redirección del dispositivo Bloomberg Keyboard Audio. En vez de ello, un nuevo dispositivo está disponible. Si utiliza Desktop Viewer, este dispositivo se denomina Bloomberg Keyboard Features. La redirección de este dispositivo proporciona las teclas Bloomberg especializadas a la sesión.

Habilitar la funcionalidad para teclados Bloomberg solo afecta a las teclas Bloomberg especializadas y al dispositivo de audio. Esto es porque las teclas normales y el lector de huellas digitales se utilizan de la misma manera que cuando la funcionalidad no está habilitada.

### Redirigir dispositivos USB de HDX Plug and Play

La redirección de dispositivos USB de HDX Plug and Play permite la redirección dinámica de dispositivos multimedia al servidor. Los dispositivos multimedia incluyen cámaras, escáneres, reproductores multimedia y dispositivos de punto de venta (POS). Al mismo tiempo, se puede impedir la redirección de todos los dispositivos o de una parte. Modifique las directivas en el servidor o aplique directivas de grupo en el dispositivo de usuario para configurar los parámetros de la redirección. Para obtener más información, consulte Consideraciones sobre unidades del cliente y USB en la documentación de Citrix Virtual Apps and Desktops.

> **Importante:**
>
> Si se prohíbe la redirección de dispositivos USB Plug-n-Play en una directiva de servidor, el usuario no podrá supeditar dicha configuración de directiva.

Un usuario puede definir permisos en la aplicación Citrix Workspace para permitir o rechazar siempre la redirección de dispositivos, o bien para que se le notifique cada vez que se conecta un dispositivo. El parámetro solo afecta a los dispositivos que se conectan después de que el usuario cambia el parámetro.

### Para asignar un puerto COM del cliente a un puerto COM del servidor

La asignación de puertos COM del cliente permite utilizar los dispositivos conectados a los puertos COM del dispositivo de usuario durante las sesiones. Estas asignaciones se pueden utilizar de la misma forma que cualquier otra asignación de red.

Es posible asignar puertos COM de cliente desde una interfaz de comandos. También se puede controlar la asignación de puertos COM de cliente desde la herramienta Configuración de Escritorio remoto (Servicios de Terminal Server) o a través de directivas. Para obtener información sobre las directivas, consulte la documentación de Citrix Virtual Apps and Desktops.

> **Importante:**
>
> La asignación de puertos COM no es compatible con TAPI.

1. En implementaciones de Citrix Virtual Apps and Desktops, habilite la configuración de directiva Redirección de puertos COM del cliente.
2. Inicie sesión en la aplicación Citrix Workspace.
3. Escriba lo siguiente en una interfaz de comandos:

   ```
   net use comx: \\\\client\\comz:
   ```

   Donde:

   - x es el número del puerto COM en el servidor (los puertos del 1 al 9 se pueden asignar)
   - z es el número del puerto COM del cliente que quiere asignar

4. Para confirmar la operación, escriba:

   ```
   net use
   ```

   El mensaje muestra las unidades asignadas, los puertos LPT y los puertos COM asignados.

Para utilizar este puerto COM en una sesión de aplicación o escritorio virtual, instale el dispositivo con el nombre asignado. Por ejemplo, si asigna COM1 en el cliente a COM5 en el servidor, instale el dispositivo de puerto COM en COM5 durante la sesión. Utilice este puerto COM asignado del mismo modo que lo haría con un puerto COM del dispositivo del usuario.

#### Configurar el sonido USB

> **Nota:**
>
> - Si instala o actualiza la versión de la aplicación Citrix Workspace para Windows por primera vez, agregue los archivos de plantilla más recientes al GPO local. Para obtener más información sobre cómo agregar los archivos de plantilla al GPO local, consulte Plantilla administrativa de objeto de directiva de grupo. Para la actualización de versiones, los parámetros existentes se conservan al importar los archivos más recientes.
> - Esta función solo está disponible en el servidor Citrix Virtual Apps.

**Para configurar dispositivos de audio USB:**

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Workspace > Experiencia de usuario** y seleccione **Audio a través de redirección de USB genérico**.
3. Modifique los parámetros.
4. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**
5. Abra el símbolo del sistema en modo de administrador.
6. Ejecute este comando:
   `gpupdate /force`.

#### Dispositivos de almacenamiento masivo

Solo en el caso de dispositivos de almacenamiento masivo, además de la compatibilidad con USB, el acceso remoto está disponible a través de la asignación de unidades del cliente. Puede configurarlo a través de la directiva de la aplicación Citrix Workspace para Windows **Uso remoto de dispositivos cliente** > **Asignación de unidades del cliente**. Al aplicar esta directiva, cuando los usuarios inician sesión, las unidades del dispositivo del usuario se asignan automáticamente a las letras de las unidades del escritorio virtual. Las unidades se muestran como carpetas compartidas con letras de unidades asignadas.

Las principales diferencias entre los dos tipos de directivas de comunicación remota son las siguientes:

| Función | Asignación de unidades del cliente | Compatibilidad con USB |
|---|---|---|
| Habilitada de forma predeterminada | Sí | No |
| Configuración para acceso de solo lectura | Sí | No |
| Dispositivo para quitar con seguridad durante una sesión | No | Sí, si un usuario hace clic en Quitar hardware con seguridad en el área de notificaciones |

Si habilita las directivas “USB genérico” y “Asignación de unidades del cliente”, e inserta un dispositivo de almacenamiento masivo antes del inicio de una sesión, ese dispositivo se redirigirá primero mediante la asignación de unidades del cliente, antes de tenerse en cuenta para la redirección de USB genérico. Si se inserta después del inicio de una sesión, se redirigirá a través de la compatibilidad con USB antes de la asignación de unidades del cliente.

### Asignación de unidades de cliente

La asignación de unidades del cliente admite la transferencia de datos entre el host y el cliente como un flujo. La transferencia de archivos se adapta a las condiciones cambiantes de rendimiento de la red. También utiliza cualquier ancho de banda adicional disponible para ampliar la velocidad de la transferencia de datos.

De manera predeterminada, esta función está habilitada.

Para inhabilitar esta función, configure así la siguiente clave de Registro y reinicie el servidor:

Ruta: `HKEY_LOCAL_MACHINE\System\Currentcontrolset\services\picadm\Parameters`
Nombre: `DisableFullStreamWrite`
Tipo: REG_DWORD
Valor:
`0x01` = función inhabilitada
`0` o ningún valor = función habilitada

La aplicación Citrix Workspace para Windows admite la asignación de dispositivos en los dispositivos de usuario de manera que estén disponibles desde una sesión. Los usuarios pueden:

- Tener acceso imperceptible a las unidades locales, impresoras y puertos COM.

- Cortar y pegar entre sesiones y el portapapeles de Windows local.
- Escuchar sonido (sonidos del sistema y archivos WAV) reproducido en la sesión.

La aplicación Citrix Workspace informa al servidor sobre las unidades cliente, los puertos COM y los puertos LPT disponibles. De forma predeterminada, a las unidades del cliente se les asignan letras de unidad del servidor y se crean colas de impresión de servidor para impresoras cliente, por lo que parece que estén directamente conectadas a la sesión. Estas asignaciones están disponibles solamente para el usuario durante la sesión actual. Se las elimina cuando el usuario cierra la sesión y se vuelven a crear la próxima vez que el usuario inicia una sesión.

Puede usar las configuraciones de directiva de redirección de Citrix para asignar los dispositivos de usuario que no se hayan asignado automáticamente al iniciar la sesión. Para obtener más información, consulte la documentación de Citrix Virtual Apps and Desktops.

#### Inhabilitar asignaciones de dispositivos de usuario

Es posible configurar las opciones de asignación de dispositivos de usuario para controladores, impresoras y puertos con la herramienta **Administrador del servidor de Windows**. Para obtener más información sobre las opciones disponibles, consulte la documentación de Servicios de Escritorio remoto.

#### Redirigir carpetas del cliente

La redirección de carpetas del cliente cambia el modo en que los archivos del lado del cliente son accesibles desde la sesión en el host. Al habilitar solamente la asignación de unidades del cliente en el servidor, se asignan automáticamente volúmenes completos del cliente a las sesiones como enlaces UNC (Universal Naming Convention). Al habilitar la redirección de carpetas del cliente en el servidor y el usuario la configura en el dispositivo de usuario, se redirige la parte del volumen local que especifique el usuario.

Solo las carpetas especificadas por el usuario aparecerán como enlaces UNC dentro de las sesiones, en lugar de aparecer todo el sistema de archivos del dispositivo del usuario. Si se inhabilitan los enlaces UNC mediante el Registro, las carpetas del cliente aparecen como unidades asignadas dentro de la sesión. Para obtener más información y conocer cómo configurar la redirección de carpetas del cliente para los dispositivos de usuario, consulte la documentación de Citrix Virtual Apps and Desktops.

#### Asignar unidades del cliente a letras de unidad del host

La asignación de unidades del cliente redirige letras de unidad del host a unidades existentes en el dispositivo del usuario. Por ejemplo, la unidad H de una sesión de usuario Citrix se puede asignar a la unidad C del dispositivo del usuario que ejecuta la aplicación Citrix Workspace para Windows.

La asignación de unidades del cliente está incorporada de forma imperceptible en las funciones estándar de redirección de dispositivos de Citrix. Para el Administrador de archivos, el Explorador de Windows y sus aplicaciones se ven como cualquier otra asignación de red.

El servidor que aloja las aplicaciones y los escritorios virtuales se puede configurar durante la instalación para que asigne unidades del cliente automáticamente a un grupo determinado de letras de unidad. La instalación predeterminada asigna letras de unidad a las unidades del cliente comenzando por la V y letras subsiguientes en orden descendente, asignando una letra de unidad a cada unidad de disco fija y de CD-ROM (a las unidades de disquete se les asignan las letras de unidad existentes). Este método da como resultado las siguientes asignaciones de unidad en la sesión:

| Letra de unidad del cliente | Accesible por el servidor como: |
|---|---|
| A | A |
| B | B |
| C | V |
| D | U |

El servidor se puede configurar para que sus respectivas letras de unidad no entren en conflicto con las del cliente. Por lo tanto, las letras de unidad del servidor se cambian a letras de unidad posteriores. En este ejemplo, si se cambian las unidades C y D del servidor por M y N, respectivamente, los equipos cliente pueden acceder a sus unidades C y D directamente. Este método proporciona las siguientes asignaciones de unidad en una sesión:

| Letra de unidad del cliente | Accesible por el servidor como: |
|---|---|
| A | A |
| B | B |
| C | C |
| D | D |

La letra de unidad utilizada para sustituir la unidad C del servidor se define durante la configuración. El resto de las letras de unidad de disco duro y de CD-ROM se sustituyen por letras de unidad secuenciales (por ejemplo; C > M, D > N, E > O). Estas letras de unidad no deben entrar en conflicto con otras asignaciones de unidad de red existentes. Si asigna la unidad de red a la misma letra de unidad que la de un servidor, la asignación de unidad de red no es válida.

Al conectar un dispositivo de usuario con un servidor, se restablecen las asignaciones del cliente a

menos que la asignación automática de dispositivos del cliente esté inhabilitada. La asignación de unidades del cliente está habilitada de forma predeterminada. Para cambiar esta configuración, use la herramienta de Configuración de Servicios de Escritorio remoto (Servicios de Terminal Server). Es también posible usar directivas para tener mayor control sobre cómo se aplica la asignación de dispositivos del cliente. Para obtener más información sobre las directivas, consulte la documentación de Citrix Virtual Apps and Desktops.

### Iniciar vPrefer

En versiones anteriores, puede especificar que se iniciara preferentemente la instancia de una aplicación instalada en el VDA (denominada “instancia local” en este documento) antes que la aplicación publicada. Para ello, configuraba el atributo KEYWORDS:prefer=”application” en **Citrix Studio**.

A partir de la versión 4.11, en casos de doble salto (en los que la aplicación Citrix Workspace se ejecuta en el VDA que aloja la sesión), ya puede controlar si la aplicación Citrix Workspace inicia:

- La instancia local de una aplicación instalada en el VDA (si está disponible como aplicación local)
- O una instancia alojada de la aplicación

vPrefer está disponible en StoreFront 3.14, Citrix Virtual Desktops 7.17 y versiones posteriores.

Al iniciar la aplicación, la aplicación Citrix Workspace lee los datos de los recursos presentes en el servidor de StoreFront y aplica la configuración en función del indicador **vPrefer** en el momento de la enumeración. La aplicación Citrix Workspace busca la ruta de instalación de la aplicación en el Registro de Windows del VDA. Si está presente, inicia la instancia local de la aplicación. De lo contrario, se inicia una instancia alojada de la aplicación.
Si inicia una aplicación que no está en el VDA, la aplicación Citrix Workspace inicia la aplicación alojada. Para obtener más información sobre cómo StoreFront gestionaba el inicio local, consulte Controlar el inicio de aplicaciones locales en escritorios publicados en la documentación de Citrix Virtual Apps and Desktops.

Si no quiere que la instancia local de la aplicación se inicie en el VDA, establezca **LocalLaunchDisabled** en **True** mediante PowerShell en el Delivery Controller. Para obtener más información, consulte la documentación de Citrix Virtual Apps and Desktops.

Esta función ayuda a iniciar aplicaciones más rápido, proporcionando así una mejor experiencia de usuario. Puede configurarla mediante la plantilla administrativa del objeto de directiva de grupo (GPO). De forma predeterminada, vPrefer se habilita solo en una situación de doble salto.

> **Nota:**
>
> Si instala o actualiza la versión de la aplicación Citrix Workspace por primera vez, agregue los archivos de plantilla más recientes al GPO local. Para obtener más información sobre cómo agregar los archivos de plantilla al GPO local, consulte Plantilla administrativa de objeto de directiva

> de grupo. Para la actualización de versiones, los parámetros existentes se conservan al importar los archivos más recientes.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Autoservicio**.
3. Seleccione la directiva **vPrefer**.
4. Seleccione **Enabled**.
5. En la lista desplegable **Permitir aplicaciones**, seleccione una de estas opciones:
   - **Permitir todas las aplicaciones:** Esta opción inicia la instancia local de todas las aplicaciones presentes en el VDA. La aplicación Citrix Workspace busca la aplicación instalada, incluidas las aplicaciones nativas de Windows, como el Bloc de notas, la Calculadora, WordPad y el símbolo del sistema. A continuación, inicia la aplicación en el VDA en lugar de iniciarla en la aplicación alojada.
   - **Permitir aplicaciones instaladas:** Esta opción inicia la instancia local de las aplicaciones instaladas que haya presentes en el VDA. Si la aplicación no está instalada en el VDA, se inicia la aplicación alojada. De forma predeterminada, se selecciona la opción **Permitir aplicaciones instaladas** cuando se **habilita** la directiva **vPrefer**. Esta opción excluye las aplicaciones nativas del sistema operativo Windows, como el Bloc de notas y la Calculadora, entre otras.
   - **Permitir aplicaciones de red:** Esta opción inicia la instancia de una aplicación que esté publicada en una red compartida.
6. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**
7. Vuelva a iniciar la sesión para que los cambios surtan efecto.

**Limitación:**

- Workspace para Web no admite esta función.

## Configuración de Workspace

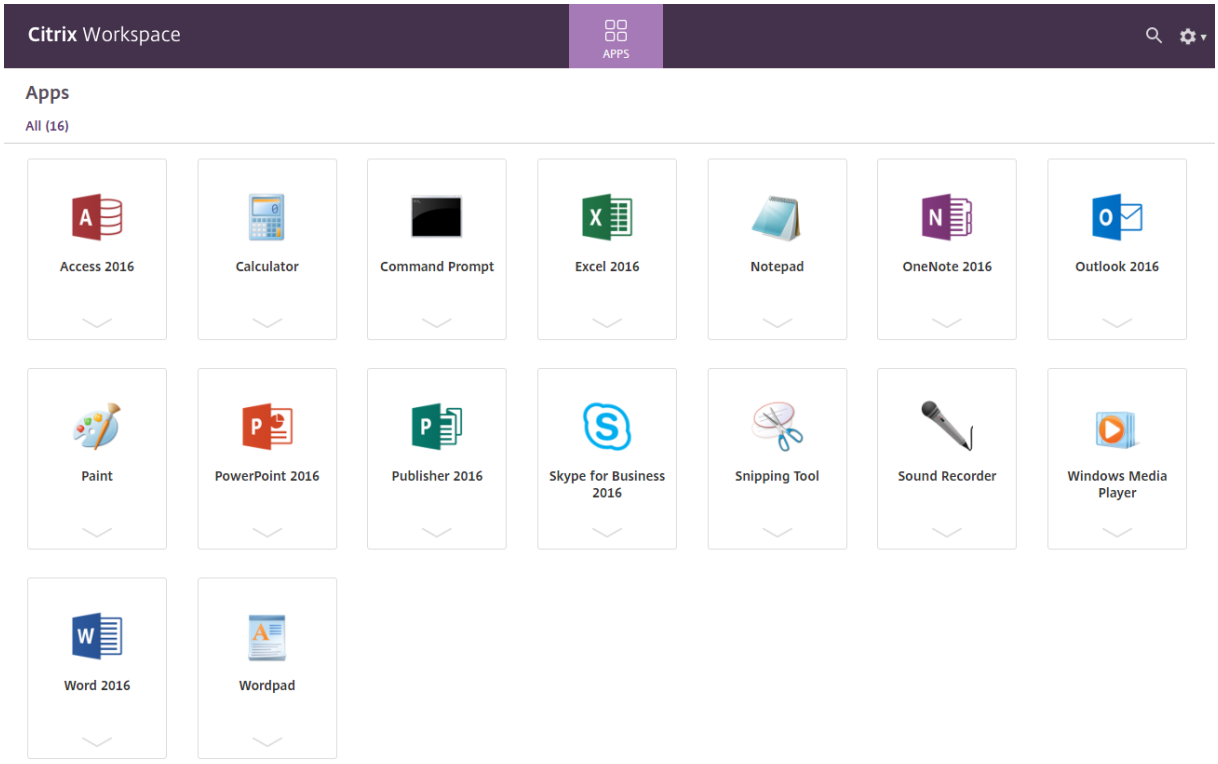
La aplicación Citrix Workspace para Windows admite la configuración de Workspace para los suscriptores, que pueden estar usando uno o varios servicios disponibles en Citrix Cloud.

La aplicación Citrix Workspace muestra de forma inteligente solamente los recursos específicos del espacio de trabajo a los que tienen derecho los usuarios. Todos los recursos del espacio de trabajo digital disponibles en la aplicación Citrix Workspace son alimentados por el servicio de experiencia de Citrix Cloud Workspace.

Un espacio de trabajo (Workspace) forma parte de una solución de espacio de trabajo digital que permite a los departamentos de TI entregar de manera segura un acceso a aplicaciones desde cualquier dispositivo.

Esta captura de pantalla es un ejemplo de un espacio de trabajo tal y como lo ven los suscriptores. El diseño de esta interfaz está evolucionando y es posible que no sea exactamente igual a la interfaz que estén usando actualmente sus suscriptores. Por ejemplo, puede figurar “StoreFront” en la parte superior de la página en lugar de “Workspace”.




## Integración de Content Collaboration Service

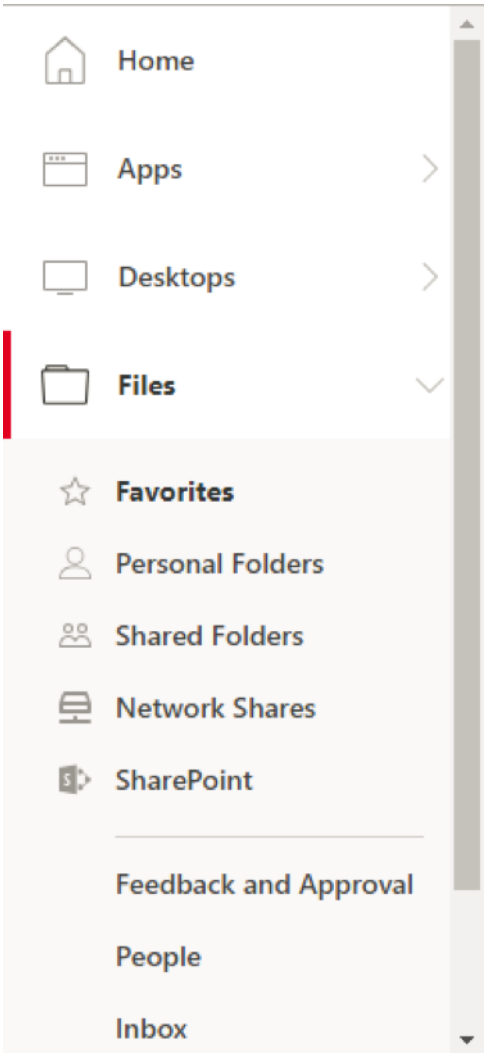
Esta versión presenta la integración de Citrix Content Collaboration Service en la aplicación Citrix Workspace. Citrix Content Collaboration permite intercambiar documentos de manera fácil y segura, enviar documentos grandes por correo electrónico, gestionar de forma segura las transferencias de documentos a terceros y acceder a un espacio de colaboración. Citrix Content Collaboration ofrece muchas maneras de trabajar, incluida una interfaz web, clientes móviles, aplicaciones de escritorio e integración con Microsoft Outlook y Gmail.

Puede acceder a la funcionalidad Citrix Content Collaboration desde la aplicación Citrix Workspace. Para ello, vaya a la ficha **Archivos** que se muestra en la aplicación Citrix Workspace. La ficha **Archivos** solo se ve si Content Collaboration está habilitado en la configuración de Workspace, en la consola de Citrix Cloud.

> **Nota:**
>
> La integración de Citrix Content Collaboration en la aplicación Citrix Workspace no se admite en Windows Server 2012 ni 2016 debido a una opción de seguridad del sistema operativo.

En esta imagen se muestra el contenido de ejemplo de la ficha **Archivos** de la nueva aplicación Citrix Workspace:




**Limitaciones:**

- Restablecer la aplicación Citrix Workspace no hace que se cierre la sesión de Citrix Content Collaboration.
- Cambiar de almacén en la aplicación Citrix Workspace no hace que Citrix Content Collaboration cierre la sesión.

**Configurar la ubicación de descarga para Citrix Files mediante el Editor del Registro:**

1. Abra el Editor del Registro y vaya a `HKEY_CURRENT_USER\Software\Citrix\Dazzle\`.
2. Cree una clave de valor de cadena llamada **DownloadPreference**.
3. Copie y pegue la ruta de descarga deseada para Citrix Files en la columna Valor.
4. Si quiere una solicitud para cada descarga, establezca la columna Valor en *.

Para obtener información sobre la configuración de la ubicación de descarga de los Citrix Files me-

diante el cuadro de interfaz de usuario **Preferencias avanzadas**, consulte Configurar la ubicación de descarga mediante Preferencias avanzadas en la documentación de ayuda de la aplicación Citrix Workspace para Windows.

### Aplicaciones SaaS

El acceso seguro a las aplicaciones SaaS ofrece una experiencia de usuario unificada en la entrega de aplicaciones SaaS publicadas a los usuarios. Las aplicaciones SaaS están disponibles con el inicio Single Sign-On. Ahora los administradores pueden proteger la red de la organización y los dispositivos de los usuarios finales frente al malware y las filtraciones de datos. Para ello, los administradores filtran el acceso a sitios web y categorías de sitios web específicos.

La aplicación Citrix Workspace para Windows admite el uso de aplicaciones SaaS con Citrix Secure Private Access. Este servicio permite a los administradores proporcionar una experiencia coherente, con Single Sign-On e inspección de contenido.

La entrega de aplicaciones SaaS desde la nube presenta los siguientes beneficios:

- Configuración simple: Fácil de operar, actualizar y consumir.
- Single Sign-On: Inicio de sesión sin complicaciones gracias a Single Sign-On.
- Plantilla estándar para aplicaciones diferentes: Configuración basada en plantillas para las aplicaciones de uso extendido.

La aplicación Citrix Workspace inicia las aplicaciones SaaS en Citrix Enterprise Browser (antes denominado Citrix Workspace Browser). Para obtener información, consulte la documentación de Citrix Enterprise Browser.

**Limitaciones:**

1. Cuando inicia una aplicación publicada con la opción de impresión habilitada y la descarga inhabilitada, y emite un comando de impresión en una aplicación iniciada, aún puede guardar el PDF. Como solución temporal, para inhabilitar estrictamente la funcionalidad de descarga, inhabilite la opción de impresión.
2. Es posible que los vídeos incrustados en una aplicación no funcionen.

Para obtener más información sobre cómo configurar espacios de trabajo, consulte Configurar el espacio de trabajo en Citrix Cloud.

### Impresión de PDF

La aplicación Citrix Workspace para Windows admite la impresión de documentos PDF durante las sesiones. El controlador de impresora universal PDF de Citrix (o Citrix PDF Universal Printer) permite imprimir documentos abiertos con aplicaciones alojadas o aplicaciones ejecutadas en Citrix Virtual Apps and Desktops y Citrix DaaS.

Cuando un usuario selecciona la opción **Citrix PDF Printer** en el cuadro de diálogo **Print**, el controlador convierte el archivo a documento PDF y lo transfiere al dispositivo local. El PDF se abre con el visor de PDF predeterminado para consultarlo y se imprime en una impresora conectada localmente.

Citrix recomienda el explorador Google Chrome o Adobe Acrobat Reader para ver documentos PDF.

Puede habilitar la impresión de PDF de Citrix mediante Citrix Studio en el Delivery Controller.

**Requisitos previos:**

- Citrix Virtual Apps and Desktops 7 1808 o una versión más reciente.
- Debe haber instalado al menos un visor de PDF en el equipo.

**Para habilitar la impresión de documentos PDF:**

1. En el Delivery Controller, use Citrix Studio para seleccionar el nodo **Directiva** en el panel de la izquierda. Puede crear una directiva o modificar una existente.
2. Habilite la directiva **Crear automáticamente la impresora universal de PDF**.

Reinicie la sesión de la aplicación Citrix Workspace para que los cambios surtan efecto.

**Limitación:**

- El explorador Microsoft Edge no admite la visualización ni la impresión de documentos PDF.

#### Modo de tableta expandida en Windows 10 cuando se usa Windows Continuum

Windows Continuum es una función de Windows 10 que se adapta al uso que se le da al dispositivo cliente. La aplicación Citrix Workspace para Windows admite el uso de Windows Continuum, incluido el cambio dinámico de modo.

Para los dispositivos cliente táctiles, el VDA de Windows 10 se inicia en modo tableta cuando no hay teclado ni mouse conectados. En cambio, se inicia en modo escritorio cuando se le conecta un teclado, un mouse o ambos. Cuando se conecta o se desconecta el teclado a cualquier dispositivo cliente, o se conecta o desconecta la pantalla en un dispositivo 2-en-1 (como Surface Pro), el modo pasa de tableta a escritorio y viceversa. Para obtener más información, consulte Modo tableta para dispositivos de pantalla táctil en la documentación de Citrix Virtual Apps and Desktops.

En un dispositivo cliente con función táctil, el VDA de Windows 10 detecta la presencia de un teclado o un mouse cuando se conecta o se reconecta a una sesión. También detecta cuando se conecta o desconecta un teclado o mouse durante la sesión. Esta función está habilitada de forma predeterminada. Para inhabilitar la función, modifique la directiva **Cambiar modo tableta** mediante Citrix Studio.

El modo tableta ofrece una interfaz de usuario que se adapta mejor a las pantallas táctiles:

- Botones ligeramente más grandes.
- La pantalla **Inicio** y todas las aplicaciones que inicie se abren en modo de pantalla completa.

- La barra de tareas incluye un botón Atrás.
- Los iconos desaparecen de la barra de tareas.

El modo escritorio ofrece la interfaz de usuario tradicional, donde se interactúa de la misma manera que con un PC con teclado y mouse.

> **Nota:**
>
> Workspace para Web no admite la función Windows Continuum.

### Redirección de contenido del explorador web

Redirigir el contenido del explorador web impide que las páginas web incluidas en la lista de permitidos se generen en el lado del agente VDA. Esta función utiliza la aplicación Citrix Workspace para crear una instancia de motor de generación correspondiente en el lado del cliente, que obtiene el contenido HTTP y HTTPS a partir de la URL.

> **Nota:**
>
> Puede especificar que las páginas web se redirijan al lado del VDA (no al lado del cliente) mediante una lista de bloqueados.

La redirección de contenido del explorador web admite el explorador Google Chrome, además del explorador Internet Explorer. La redirección de contenido del explorador web redirige el contenido de un explorador web a un dispositivo cliente, y crea un explorador web correspondiente incrustado en la aplicación Citrix Workspace. Esta función reduce el uso de red, el procesamiento de páginas y los gráficos que aparecen en el dispositivo de punto final. Por tanto, mejora la experiencia del usuario cuando este navega por páginas web con contenido sofisticado, especialmente aquellas páginas web que contienen vídeos HTML5 o WebRTC.

- Las cookies persisten en todas las sesiones: al salir de un explorador y al volver a iniciarlo, no se le pedirá que vuelva a introducir sus credenciales.
- Ahora los exploradores web respetan el idioma del sistema local.

Para obtener más información, consulte Redirección de contenido de explorador web.

#### Configurar la ruta para el almacenamiento de datos temporales del explorador web superpuesto de la redirección de contenido del explorador web

A partir de la versión 2303 de la aplicación Citrix Workspace, se le solicita que configure la ruta de almacenamiento de datos temporales para el explorador web basado en el Chromium Embedded Framework (CEF). Para configurar la ruta, haga lo siguiente:

1. Abra el Editor del Registro.
2. Vaya a la ruta del Registro `HKCU\Software\Citrix\HdxMediaStream`.

3. Cree un valor del Registro con estos atributos:
    - Nombre de la clave del Registro: `BCRProfilePath`
    - Valor del Registro: Cadena `<folder for CEF based BCRtmp files>`
4. Reinicie la aplicación Citrix Workspace para que los cambios surtan efecto.

## Citrix Analytics

La aplicación Citrix Workspace está equipada para transmitir registros de manera segura a Citrix Analytics. Los registros se analizan y almacenan en los servidores de Citrix Analytics cuando está habilitado. Para obtener más información sobre Citrix Analytics, consulte Citrix Analytics.

### Mejora en Citrix Analytics Service

Con esta versión, la aplicación Citrix Workspace está destinada a transmitir de forma segura la dirección IP pública del salto de red más reciente a Citrix Analytics Service. Estos datos se recopilan por inicio de sesión. Ayuda a Citrix Analytics Service a analizar si los problemas de rendimiento deficiente están vinculados a áreas geográficas específicas.

De forma predeterminada, los registros de direcciones IP se envían a Citrix Analytics Service. Sin embargo, puede inhabilitar esta opción en la aplicación Citrix Workspace mediante el Editor del Registro.

Para inhabilitar las transmisiones de registros de direcciones IP, vaya a la siguiente ruta del Registro y **desactive** la clave `SendPublicIPAddress`.

- En máquinas con Windows de 64 bits, vaya a: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle`.
- En máquinas con Windows de 32 bits, vaya a: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`.

> **Nota:**
>
> - Las transmisiones de direcciones IP se producen en el mejor de los casos. Aunque la aplicación Citrix Workspace transmite todas las direcciones IP en las que se inicia, es posible que algunas de las direcciones no sean exactas.
> - En entornos de clientes cerrados, donde los dispositivos de punto final operan dentro de una intranet, compruebe que la URL `https://locus.analytics.cloud.com/api/locateip` se halla en la lista de permitidos del dispositivo de punto final en cuestión.

La aplicación Citrix Workspace está diseñada para transmitir datos de forma segura a Citrix Analytics Service desde sesiones ICA que se inician desde un explorador web.

Para obtener más información sobre cómo utiliza esta información Performance Analytics, consulte Self-Service Search for Performance.

### Mouse relativo

La función "mouse relativo" determina hasta dónde se ha movido el cursor desde el último fotograma de una ventana o pantalla.
El mouse relativo utiliza las diferencias píxeles entre los movimientos del cursor. Por ejemplo, cuando se cambia la dirección de la cámara mediante controles del cursor, la función registra el cambio. Las aplicaciones también suelen ocultar el cursor del mouse porque la posición del cursor en relación con las coordenadas de la pantalla no es relevante cuando se manipula una escena o un objeto 3D.

El mouse relativo ofrece una opción para interpretar la posición del mouse de un modo relativo en lugar de hacerlo de un modo absoluto. La interpretación es necesaria para las aplicaciones que exigen una entrada de mouse relativo en lugar de absoluto.

Puede configurar la función tanto por usuario como por sesión, lo que proporciona un control más detallado sobre la disponibilidad de la función.

> **Nota**
>
> Esta función solo se puede aplicar en una sesión de escritorio publicado.

La configuración de la función mediante el Editor del Registro o el archivo default.ica permite que la configuración sea persistente incluso después de finalizar la sesión.

#### Configurar el mouse relativo mediante el Editor del Registro

Para configurar la función, establezca las siguientes claves del Registro según corresponda y, a continuación, reinicie la sesión para que los cambios surtan efecto:

**Para que la función esté disponible por sesión:**
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse`

**Para que la función esté disponible por usuario:**
`HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse`

- Nombre: RelativeMouse
- Tipo: REG_SZ
- Valor: True

> **Nota:**
>
> - Los valores establecidos en el Editor del Registro tienen prioridad sobre la configuración del archivo ICA.
> - Los valores establecidos en HKEY_LOCAL_MACHINE y HKEY_CURRENT_USER deben ser los mismos. Es posible que, si hay diferentes valores, haya conflictos.

#### Configurar el mouse relativo mediante el archivo default.ica

1. Abra el archivo default.ica, ubicado normalmente en `C:\inetpub\wwwroot\Citrix\<site name>\conf\default.ica`, donde "sitename" es el nombre especificado del sitio cuando se creó. Para los clientes de StoreFront, el archivo default.ica suele estar en `C:\inetpub\wwwroot\Citrix\<Storename>\App_Data\default.ica`, donde `storename` es el nombre establecido del almacén cuando se creó.
2. Agregue una clave con el nombre RelativeMouse en la sección WFClient. Defina su valor en la misma configuración que el objeto JSON.
3. Establezca el valor según sea necesario:
   - true: Para habilitar el mouse relativo
   - false: Para inhabilitar el mouse relativo
4. Vuelva a iniciar la sesión para que los cambios surtan efecto.

> **Nota:**
>
> Los valores establecidos en el Editor del Registro tienen prioridad sobre la configuración del archivo ICA.

#### Habilitar el mouse relativo desde Desktop Viewer

1. Inicie sesión en la aplicación Citrix Workspace.
2. Lance una sesión de escritorio publicado.
3. En la barra de herramientas de Desktop Viewer, seleccione **Preferencias**.

   Aparecerá la ventana "Citrix Workspace - Preferencias".
4. Seleccione **Conexiones**.
5. En los parámetros de **Mouse relativo**, habilite **Usar mouse relativo**.
6. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**

> **Nota:**
>
> La configuración del mouse relativo desde Desktop Viewer aplica la función solo por sesión.

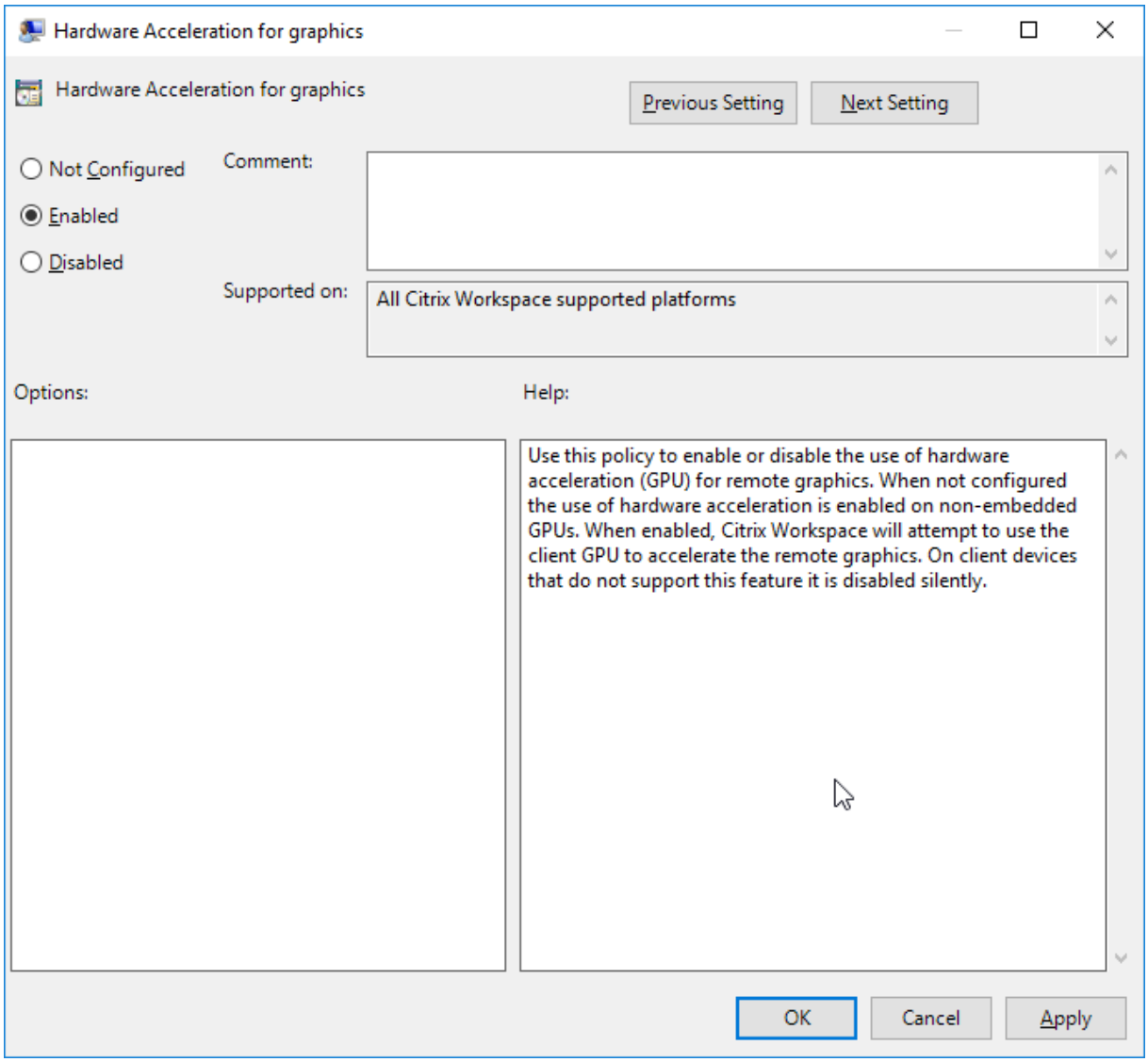
### Decodificación por hardware

Cuando se usa la aplicación Citrix Workspace (con HDX Engine 14.4), la GPU se puede usar para la decodificación H.264 donde esté disponible en el cliente. La capa de API utilizada para la decodificación por GPU es DirectX Video Acceleration.

**Para habilitar la decodificación por hardware con la plantilla administrativa de GPO de la aplicación Citrix Workspace:**

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Citrix Workspace** > **Experiencia de usuario**.
3. Seleccione **Aceleración de hardware para gráficos**.
4. Seleccione **Habilitada** y haga clic en **Aplicar** y luego en **Aceptar**.




Para validar si la directiva está configurada y si se utiliza la aceleración de hardware para sesiones ICA activas, compruebe estas entradas del Registro:

Ruta del Registro: `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\CEIP\Data\GfxRender`.

> **Sugerencia**
>
> El valor de **Graphics_GfxRender_Decoder** y **Graphics_GfxRender_Renderer** debe ser 2. Si el valor es 1, esto significa que se está usando la decodificación por CPU.

Cuando use la función de decodificación por hardware, tenga en cuenta que existen las limitaciones siguientes:

- Si el cliente tiene dos unidades GPU y uno de los monitores está activo en la segunda GPU, se usa la decodificación basada en CPU.
- Al conectarse a un servidor de Citrix Virtual Apps con Windows Server 2008 R2, no use la decodificación por hardware en el dispositivo Windows del usuario. Si se habilita, pueden observarse problemas, como un rendimiento lento al resaltar texto y un parpadeo de pantalla.

### Entrada de micrófono

La aplicación Citrix Workspace admite varias entradas de micrófono en el cliente. Puede usar micrófonos instalados localmente para:

- Actividades en tiempo real, como llamadas desde sistemas de telefonía integrada en el equipo y conferencias web.
- Aplicaciones de grabación en el servidor, como programas de dictado.
- Grabaciones de vídeo y sonido.

Los usuarios de la aplicación Citrix Workspace pueden seleccionar si quieren usar los micrófonos conectados a sus dispositivos mediante un parámetro en la Central de conexiones. Los usuarios de Citrix Virtual Apps and Desktops y Citrix DaaS también pueden usar las Preferencias del visor de Citrix Virtual Apps and Desktops y Citrix DaaS para inhabilitar sus micrófonos y cámaras web.

### Admitir varios monitores

Puede usar un máximo de ocho monitores con la aplicación Citrix Workspace para Windows.

Cada monitor en una configuración de varios monitores tiene su propia resolución, configurada por el fabricante. Los monitores pueden ofrecer diferentes resoluciones y orientaciones durante las sesiones.

Las sesiones pueden distribuirse entre varios monitores de dos formas:

- En modo de pantalla completa, con varios monitores en la sesión; las aplicaciones se presentan en los monitores como lo harían localmente.

  **Citrix Virtual Apps and Desktops y Citrix DaaS:** Puede mostrar la ventana de Desktop Viewer en cualquier subconjunto de rectángulos de monitores; para ello, cambie el tamaño de la ventana en cualquier parte de esos monitores y haga clic en **Maximizar**.

- En modo de ventana, con la imagen de un solo monitor para la sesión; las aplicaciones no se acoplan a monitores individuales.

**Citrix Virtual Apps and Desktops y Citrix DaaS:** Cuando posteriormente se inicia cualquier escritorio en la misma asignación (anteriormente "grupo de escritorios"), se mantiene el parámetro de ventana y se muestra el escritorio en los mismos monitores. En la medida en que la distribución de monitores sea rectangular, se pueden mostrar varios escritorios virtuales en un dispositivo. Si la sesión de aplicaciones y escritorios virtuales usa el monitor principal en el dispositivo, este será el monitor principal de la sesión. De lo contrario, el monitor con el número más bajo en la sesión se convierte en el monitor principal.

Para habilitar la compatibilidad con varios monitores, compruebe lo siguiente:

- El dispositivo de usuario está configurado para admitir el uso de varios monitores.
- El sistema operativo puede detectar cada uno de los monitores. En plataformas con Windows, para verificar que esta detección tiene lugar, vaya a **Configuración** > **Sistema**, haga clic en **Pantalla** y confirme que cada monitor aparezca por separado.
- Después de detectar los monitores:
  - **Citrix Virtual Desktops:** Defina el límite de memoria gráfica con la configuración **Límite de memoria de presentación** de las directivas de máquina de Citrix.
  - **Citrix Virtual Apps:** Según la versión del servidor de Citrix Virtual Apps que haya instalado:
    - Defina el límite de memoria de gráficos con la configuración Límite de memoria de presentación en la **directiva de equipo de Citrix**.
    - En la consola de administración de Citrix para el servidor de Citrix Virtual Apps, seleccione la comunidad y, en el panel de tareas, seleccione:
      - **Modify Server Properties** > **Modify all properties** > **Server Default** > **HDX Broadcast** > **Display**
      - O **Modify Server Properties** > **Modify all properties** > **Server Default** > **ICA** > **Display**
    - Y establezca la memoria máxima que se utilizará para los gráficos de cada sesión.

Compruebe que el parámetro sea lo bastante amplio (en kilobytes) para ofrecer suficiente memoria gráfica. Si este parámetro no es lo suficientemente grande, el recurso publicado se restringirá al subconjunto de monitores que cubra el tamaño especificado.

**Uso de Citrix Virtual Desktops en monitores dobles:**

1. Seleccione Desktop Viewer y haga clic en la flecha hacia abajo.
2. Seleccione la opción **Ventana**.
3. Arrastre la pantalla Citrix Virtual Desktops entre los dos monitores. Asegúrese de que aproximadamente la mitad de la pantalla esté presente en cada monitor.
4. En la barra de herramientas de Citrix Virtual Desktops, seleccione **Pantalla completa**.

La pantalla se extiende ahora a ambos monitores.

Para calcular los requisitos de memoria gráfica para Citrix Virtual Apps and Desktops y Citrix DaaS, consulte el artículo CTX115637 en Knowledge Center.

### Impresora

Para sobrescribir los parámetros de la impresora en el dispositivo de usuario

1. En el menú **Imprimir** de la aplicación del dispositivo de usuario, elija **Propiedades**.
2. En la ficha **Parámetros del cliente**, haga clic en Optimizaciones avanzadas y modifique las opciones “Compresión de imagen” y “Almacenamiento en caché de imágenes y fuentes”.

#### Controlar el teclado en pantalla

Para habilitar el acceso táctil a aplicaciones y escritorios virtuales desde tabletas Windows, la aplicación Citrix Workspace muestra automáticamente el teclado en pantalla:

- Al activar un campo de entrada de texto
- Cuando el dispositivo está en modo tienda o tableta

En algunos dispositivos y en algunas circunstancias, la aplicación Citrix Workspace no puede detectar con precisión el modo del dispositivo. Es posible que el teclado en pantalla también aparezca cuando no quiera.

Para evitar que aparezca el teclado en pantalla al usar un dispositivo convertible:

- Cree un valor REG_DWORD DisableKeyboardPopup en `HKEY\\_CURRENT\\_USER\\SOFTWARE\\Citrix\\ICA Client\\Engine\\Configuration\\Advanced\\Modules\\MobileReceiver`
- Y establezca el valor en 1

> **Nota:**
>
> En una máquina x64, cree el valor en HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver.

Las claves se pueden configurar en estos 3 modos:

- **Automatic:** AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 0
- **Always popup** (teclado en pantalla): AlwaysKeyboardPopup = 1; DisableKeyboardPopup = 0
- **Never popup** (teclado en pantalla): AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 1

### Teclas de acceso rápido

Se pueden configurar combinaciones de teclas para que la aplicación Citrix Workspace las interprete como una funcionalidad especial. Cuando se habilita la directiva de teclas de acceso directo, se

pueden especificar las teclas de acceso directo de Citrix, el comportamiento de las teclas de acceso directo de Windows y la disposición del teclado para las sesiones.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Experiencia de usuario**.
3. Seleccione la directiva Accesos directos de teclado.
4. **Habilítela** y seleccione las opciones necesarias.
5. Reinicie la sesión de la aplicación Citrix Workspace para que los cambios surtan efecto.

**Compatibilidad de la aplicación Citrix Workspace con iconos de color de 32 bits:**

La aplicación Citrix Workspace admite iconos de color de alta densidad de 32 bits. Para proporcionar aplicaciones integradas, selecciona automáticamente la profundidad del color para:

- Las aplicaciones visibles en el cuadro de diálogo **Central de conexiones**
- El menú Inicio
- La barra de tareas

> **Precaución**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Para establecer una profundidad preferida, puede agregar una cadena de clave de Registro llamada `TWIDesiredIconColor` a `HKEY\\_LOCAL\\_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences` y establecerla en el valor necesario. Las profundidades de color posibles son 4, 8, 16, 24 y 32 bits por píxel. Si la conexión de la red es lenta, los usuarios pueden seleccionar valores de profundidad de color menores para los iconos.

### Personalizar la ubicación del acceso directo de la aplicación mediante la línea de comandos

La función de integración de accesos directos en el menú Inicio y en el escritorio solamente permite colocar los accesos directos de las aplicaciones publicadas en el menú **Inicio** de Windows y en el escritorio. No es necesario que los usuarios se suscriban a las aplicaciones desde la interfaz de usuario de Citrix Workspace. La integración del menú Inicio y la administración de accesos directos del escritorio proporcionan una experiencia de escritorio fluida para grupos de usuarios. También para los usuarios que necesitan acceder a un conjunto básico de aplicaciones de forma continua.

Esta marca se denomina **SelfServiceMode** y está establecida como `True` de forma predeterminada. Cuando el administrador establece el indicador **SelfServiceMode** en `False`, no se puede acceder a la interfaz de usuario de autoservicio. En su lugar, puede acceder a aplicaciones suscritas desde el menú Inicio y accesos directos de escritorio, lo que se conoce como modo de acceso directo solamente.

Los usuarios y los administradores pueden usar una serie de parámetros de Registro para personalizar el modo en que se configuran los accesos directos.

#### Trabajar con accesos directos

- Los usuarios no pueden quitar aplicaciones. Todas las aplicaciones son obligatorias cuando se trabaja con la marca **SelfServiceMode** establecida en False (modo de acceso directo solamente). Si quita un icono de acceso directo que hubiera en el escritorio, el icono vuelve a aparecer cuando selecciona **Actualizar** desde el icono de la aplicación Citrix Workspace situado en el área de notificaciones.
- Los usuarios solo pueden configurar un almacén. Las opciones Cuenta y Preferencias no están disponibles para evitar que el usuario configure más almacenes. El administrador puede otorgar a un usuario privilegios especiales para agregar más de una cuenta mediante la plantilla de objeto de directiva de grupo. Los administradores también pueden proporcionar privilegios especiales al agregar manualmente una clave del Registro (HideEditStoresDialog) en la máquina cliente. Cuando el administrador da este privilegio a un usuario, este usuario tiene la opción Preferencias en el icono del área de notificaciones, desde donde puede agregar y quitar cuentas.
- Los usuarios no pueden quitar las aplicaciones mediante el **Panel de control** de Windows.
- Puede agregar accesos directos de escritorio a través de un parámetro de Registro personalizable. Los accesos directos de escritorio no se agregan de forma predeterminada. Después de modificar los parámetros del Registro, reinicie la aplicación Citrix Workspace.
- Los accesos directos se crean en el menú Inicio con una ruta de categoría predeterminada, UseCategoryAsStartMenuPath.

> **Nota:**
>
> Windows 10 no permite la creación de carpetas anidadas dentro del menú Inicio. Las aplicaciones se muestran individualmente o en la carpeta raíz. No dentro de las subcarpetas de categoría que se definen con Citrix Virtual Apps.

- Puede agregar una marca [/DESKTOPDIR="Dir_name"] durante la instalación para reunir todos los accesos directos en una misma carpeta. Se admite el uso de CategoryPath para los accesos directos de escritorio.
- La función de reinstalación automática de aplicaciones modificadas se puede habilitar mediante la clave del Registro `AutoReInstallModifiedApps`. Al habilitar `AutoReInstallModifiedApps`, los cambios en los atributos de aplicaciones y escritorios publicados en el servidor se muestran

en la máquina cliente. Al inhabilitar `AutoReInstallModifiedApps`, los atributos de las aplicaciones y escritorios no se actualizan, y los accesos directos no vuelven a aparecer al actualizar si se eliminaron del cliente. De forma predeterminada, `AutoReInstallModifiedApps` está habilitada.

#### Personalizar la ubicación del acceso directo de la aplicación mediante el Editor del Registro

> **Nota:**
>
> - De forma predeterminada, las claves del Registro usan el formato de **cadena**.
> - Cambie las claves del Registro antes de configurar un almacén. Si en algún momento usted o un usuario quieren personalizar las claves del Registro, deben hacer lo siguiente:
>
> 1. Restablecer la aplicación Citrix Workspace
> 2. Configurar las claves del Registro
> 3. Y reconfigurar el almacén

#### Administrar la reconexión del control del espacio de trabajo

El control del espacio de trabajo permite que las aplicaciones sigan disponibles para los usuarios cuando estos cambian de dispositivo. Por ejemplo: el control del espacio de trabajo permite a los médicos trasladarse de una estación de trabajo a otra sin tener que reiniciar sus aplicaciones en cada dispositivo. En la aplicación Citrix Workspace, el control del espacio de trabajo en los dispositivos cliente se administra mediante la modificación del Registro. El control de Workspace también se puede realizar para los dispositivos cliente unidos a un dominio mediante la directiva de grupo.

> **Precaución:**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Cree **WSCReconnectModeUser** y modifique la clave de Registro existente **WSCReconnectMode** en la imagen maestra de escritorio o en el servidor de Citrix Virtual Apps. El escritorio publicado puede cambiar el comportamiento de la aplicación Citrix Workspace.

Parámetros posibles para la clave WSCReconnectMode de la aplicación Citrix Workspace:

- 0 = No reconectar ninguna sesión existente
- 1 = Reconectarse al iniciar una aplicación
- 2 = Reconectarse al actualizar una aplicación
- 3 = Reconectarse al iniciar o actualizar una aplicación

- 4 = Reconectarse cuando se abra la interfaz de Citrix Workspace
- 8 = Reconectarse al iniciar sesión en Windows
- 11 = Combinación de las opciones 3 y 8

#### Habilitar control del espacio de trabajo

Para inhabilitar el control del espacio de trabajo, cree la siguiente clave:

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle` (64 bits)

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\\Dazzle` (32 bits)

Nombre: **WSCReconnectModeUser**

Tipo: REG_SZ

Información del valor: `0`

Modifique la clave siguiente desde el valor predeterminado de `3` a cero

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle` (64 bits)

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle` (32 bits)

Nombre: **WSCReconnectMode**

Tipo: REG_SZ

Información del valor: `0`

> **Nota:**
>
> También puede establecer la clave **WSCReconnectAll** en false si no quiere crear una clave.

#### Claves de Registro para máquinas de 32 bits

**Clave del Registro: WSCSupported**

**Valor**: `True`

**Ruta de la clave**:

```
- HKEY_CURRENT_USER\Software\Citrix\Dazzle
- HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
  primaryStoreID +\Properties
- HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle
- HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
```

**Clave del Registro: WSCReconnectAll**

**Valor**: `True`

**Ruta de la clave**:

```
- `HKEY_CURRENT_USER\Software\Citrix\Dazzle`
- `HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
  primaryStoreID + \Properties`
- `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle`
- `HKEY_LOCAL_MACHINe\Software\Citrix\Dazzle`
```

**Clave del Registro: WSCReconnectMode**

**Valor**: 3

**Ruta de la clave**:

```
-  HKEY_CURRENT_USER\Software\Citrix\Dazzle
-  HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
   primaryStoreID +\Properties
-  HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle
-  HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
```

**Clave del Registro: WSCReconnectModeUser**

**Valor**: El Registro no se crea durante la instalación.

**Ruta de la clave**:

```
- HKEY_CURRENT_USER\Software\Citrix\Dazzle
- HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID
  +\Properties
- HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle
- HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
```

**Claves de Registro para máquinas de 64 bits:**

**Clave del Registro: WSCSupported**

**Valor**: `True`

**Ruta de la clave**:

```
- HKEY_CURRENT_USER\Software\Citrix\Dazzle
```

```
2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID
      +\Properties
3 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

**Clave del Registro: `WSCReconnectAll`**

**Valor**: `True`

**Ruta de la clave**:

```
1 -  HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 -  HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
     primaryStoreID + \Properties
3 -  HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
4 -  HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

**Clave del Registro: WSCReconnectMode**

**Valor**: 3

**Ruta de la clave**:

```
1 -  HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 -  HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
     primaryStoreID +\Properties
3 -  HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
4 -  HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

**Clave del Registro: WSCReconnectModeUser**

**Valor**: El Registro no se crea durante la instalación.

**Ruta de la clave**:

```
1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID
      +\Properties
3 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

## Desktop Viewer

Cada empresa tiene sus propias necesidades. Es posible que los requisitos para los usuarios accedan a los escritorios virtuales varíen de un usuario a otro y a medida que evolucionan las necesidades de la empresa. La experiencia de usuario al conectarse a escritorios virtuales y la medida en que el usuario puede configurar las conexiones dependen de la configuración de la aplicación Citrix Workspace para Windows.

Use **Desktop Viewer** cuando los usuarios necesiten interactuar con el escritorio virtual. El escritorio virtual del usuario pueden ser un escritorio virtual publicado, o un escritorio compartido o escritorio dedicado. En este modo de acceso, las funciones de la barra de herramientas de **Desktop Viewer** permiten al usuario abrir un escritorio virtual en una ventana, desplazar y cambiar el tamaño de ese escritorio dentro del escritorio local. Los usuarios pueden definir preferencias y trabajar en más de un escritorio mediante varias conexiones de Citrix Virtual Apps and Desktops y Citrix DaaS en el mismo dispositivo de usuario.

> **Nota:**
>
> Use la aplicación Citrix Workspace para cambiar la resolución de pantalla en los escritorios virtuales. No puede cambiar la resolución de pantalla mediante el Panel de control de Windows.

### Entrada de teclado en Desktop Viewer

En las sesiones de Desktop Viewer, la combinación de la tecla con el **logotipo de Windows** + L se transfiere al equipo local.

Ctrl+Alt+Supr se transfiere al equipo local.

Las pulsaciones de teclas que activan ciertas funciones de accesibilidad de Microsoft, como las Teclas especiales, las Teclas de filtro y las Teclas de alternancia, siempre se transfieren al equipo local.

Como una función de accesibilidad de Desktop Viewer, al presionar Ctrl+Alt+Interrumpir se muestran los botones de la barra de herramientas de **Desktop Viewer** en una ventana emergente.

Ctrl+Esc se envía al escritorio virtual remoto.

> **Nota:**
>
> De forma predeterminada, Alt+Tab transfiere el foco entre las ventanas de la sesión si Desktop Viewer está maximizado. Si Desktop Viewer se muestra en una ventana, Alt+Tab transfiere el foco entre las ventanas fuera de la sesión.

Las secuencias de teclas de acceso rápido son combinaciones de teclas diseñadas por Citrix. Las secuencias de accesos directos son, por ejemplo, la secuencia Ctrl+F1, que reproduce las teclas Ctrl+Alt+Supr, y Mayús+F2, que cambia entre el modo de pantalla completa y de ventanas en las aplicaciones.

> **Nota:**
>
> No puede usar secuencias de teclas de acceso rápido con escritorios virtuales que se muestran en Desktop Viewer, es decir, con sesiones de aplicaciones y escritorios virtuales. Sin embargo, puede usarlas con aplicaciones publicadas, es decir, con sesiones de aplicaciones virtuales.

### Escritorios virtuales

Los usuarios no pueden conectarse al mismo escritorio virtual desde una sesión de escritorio. Si el usuario lo intenta, desconecta la sesión de escritorio existente. Por lo tanto, Citrix recomienda lo siguiente:

- Los administradores no deben configurar a los clientes de un escritorio para que se conecten con un sitio que publica el mismo escritorio.
- Los usuarios no deben buscar un sitio que aloje el mismo escritorio si el sitio se configura para reconectar a los usuarios automáticamente con las sesiones existentes.
- Los usuarios no deben buscar un sitio que aloje el mismo escritorio e intentar ejecutarlo.

Un usuario que inicia una sesión localmente en un equipo que actúa como escritorio virtual bloquea la conexión con ese escritorio.

Defina la asignación de dispositivos:

- Si sus usuarios se conectan a aplicaciones virtuales, publicadas con aplicaciones virtuales, desde un escritorio virtual
- Si su organización tiene un administrador de aplicaciones virtuales independiente

La asignación de dispositivos comprueba si los dispositivos de escritorio se asignan de manera coherente en sesiones de escritorio y de aplicación. Debido a que las unidades locales se muestran como unidades de red en las sesiones de escritorio, el administrador de aplicaciones virtuales debe modificar la directiva de asignación de unidades para que incluya las unidades de red.

#### Tiempo de espera del indicador de estado

Puede cambiar el tiempo que se muestra el indicador de estado cunado el usuario inicia una sesión.

Para modificar el tiempo de espera, siga estos pasos:

1. Abra el Editor del Registro.
2. Vaya a la siguiente ruta:
    - En un sistema operativo de 64 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA CLIENT\Engine`
    - En un sistema operativo de 32 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\`
3. Cree una clave del Registro de la siguiente manera:

- Tipo: REG_DWORD
- Nombre: `SI INACTIVE MS`
- Valor: 4, si quiere que el indicador de estado desaparezca antes.

Al configurar esta clave, es posible que el indicador de estado aparezca y desaparezca a menudo. Este comportamiento es el esperado. Para suprimir el indicador de estado, haga lo siguiente:

1. Abra el Editor del Registro.
2. Vaya a la siguiente ruta:
   - En un sistema operativo de 64 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA CLIENT\`
   - En un sistema operativo de 32 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\`
3. Cree una clave del Registro de la siguiente manera:
   - Tipo: REG_DWORD
   - Nombre: `NotificationDelay`
   - Valor: Cualquier valor en milisegundos (por ejemplo, 120000)

### Tiempo de espera por inactividad para sesiones de Workspace

Los administradores pueden configurar el valor del tiempo de espera por inactividad para especificar el tiempo de inactividad permitido antes de que se cierre automáticamente la sesión de los usuarios de Citrix Workspace. Se cierra su sesión de Workspace automáticamente si el mouse, el teclado o la función táctil están inactivos durante el intervalo de tiempo especificado. El tiempo de espera por inactividad no afecta a las sesiones de aplicaciones y escritorios virtuales ni a almacenes de Citrix StoreFront que estén activos.

El valor del tiempo de espera por inactividad se puede establecer desde 1 minuto a 1440 minutos. De forma predeterminada, el tiempo de espera por inactividad no está configurado. Los administradores pueden configurar la propiedad inactivityTimeoutInMinutes mediante un módulo de PowerShell. Haga clic aquí para descargar los módulos de PowerShell de la configuración de Citrix Workspace.

La experiencia del usuario final es la siguiente:

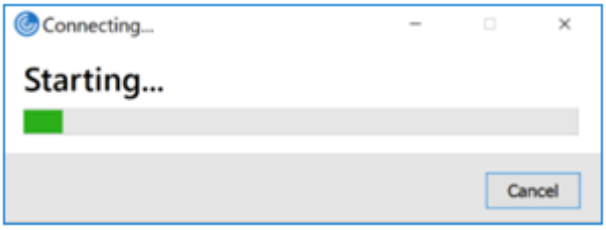
- Aparecerá una notificación en la ventana de la sesión tres minutos antes de que se le cierre la sesión, con la opción de mantener la sesión abierta o cerrar la sesión.
- La notificación aparece solamente si el valor del tiempo de espera por inactividad configurado es mayor o igual a cinco minutos.
- Los usuarios pueden hacer clic en **Mantener sesión abierta** para descartar la notificación y seguir utilizando la aplicación. En ese caso, el temporizador de inactividad se restablece a su valor configurado. También puede hacer clic en **Cerrar sesión** para finalizar la sesión del almacén actual.

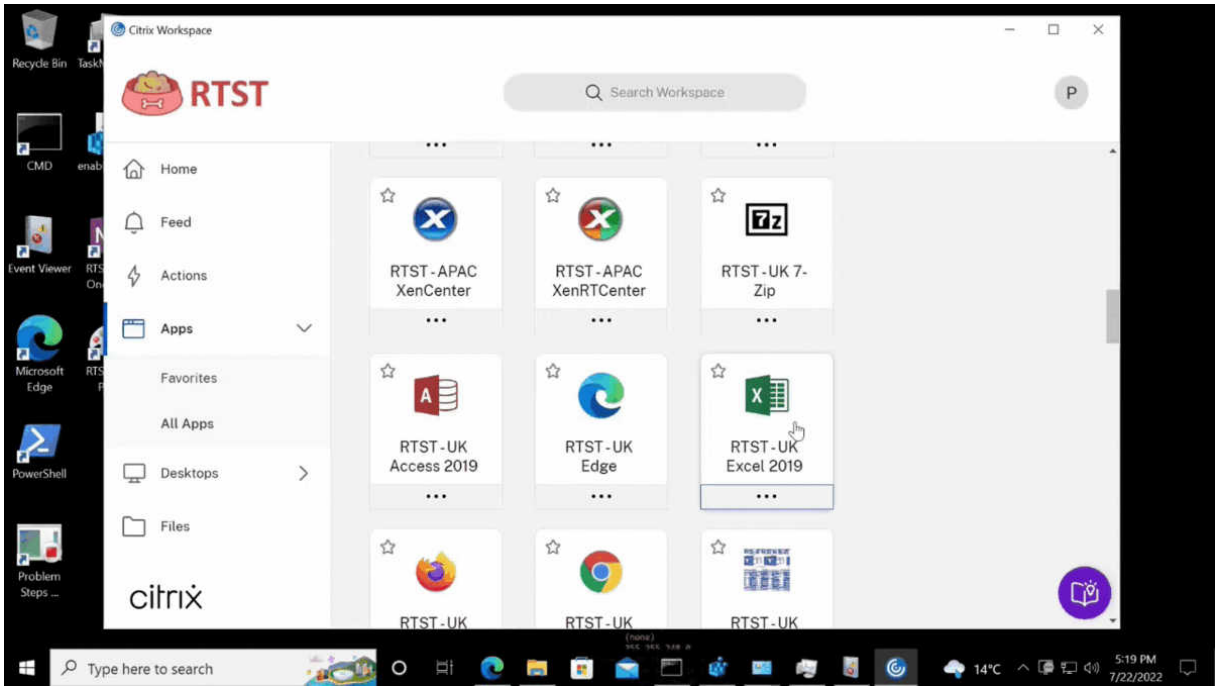
> **Nota:**
>
> Los administradores pueden configurar el tiempo de espera por inactividad solamente para sesiones de Workspace (nube).

### Experiencia mejorada al iniciar aplicaciones y escritorios virtuales [Technical Preview]

Antes, el cuadro de diálogo de progreso del inicio no era intuitivo para los usuarios. Les hacía creer que el proceso de inicio no respondía, y estos cerraban el cuadro de diálogo, ya que los mensajes de notificación eran estáticos.

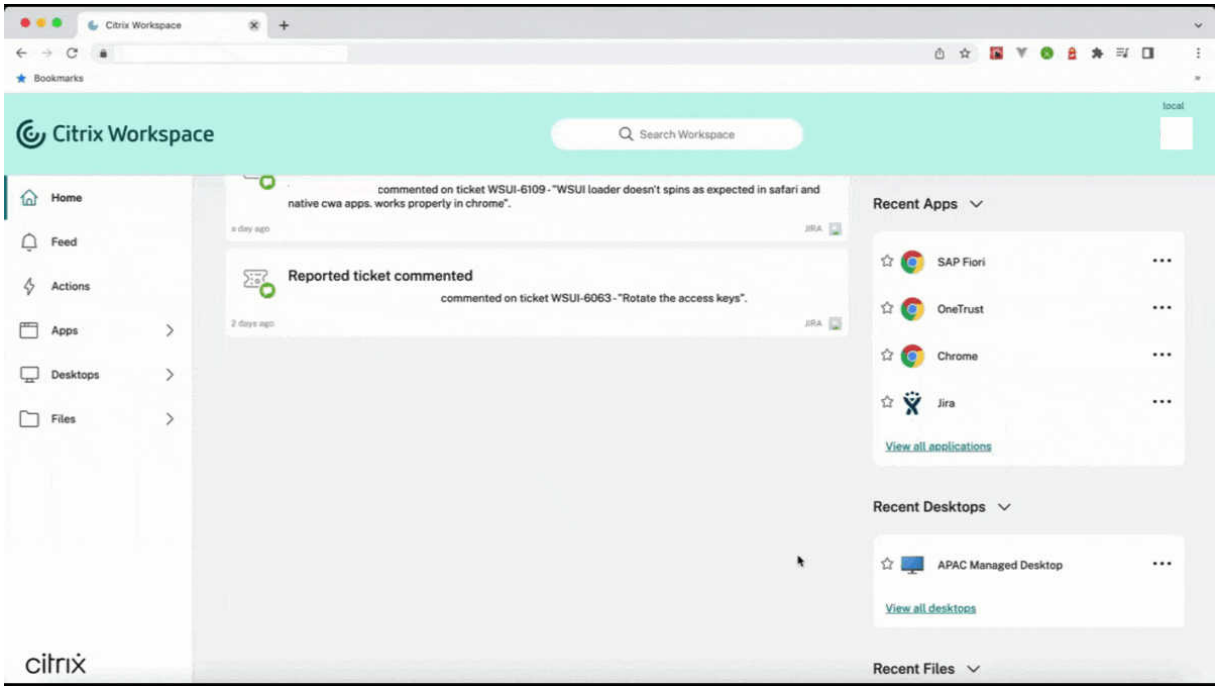



La experiencia mejorada al iniciar aplicaciones y escritorios es más informativa, moderna e intuitiva en la aplicación Citrix Workspace para Windows. Esto ayuda a mantener a los usuarios informados con datos relevantes y oportunos sobre el estado del inicio. La notificación aparece en la esquina inferior derecha de la pantalla.




Esta función también está disponible en Workspace para Web. Los usuarios pueden ver notificaciones útiles sobre el progreso del inicio en lugar de un icono giratorio solamente. Si hay un inicio en curso y el usuario intenta cerrar el explorador, aparece un mensaje de advertencia.




Puede habilitar esta función mediante el Registro:

1. Abra el Editor del Registro.
2. Vaya a `HKLM\SOFTWARE\WOW6432Node\Citrix\Dazzle`.
3. Cree y agregue una cadena del Registro con el nombre NewLaunchExpSupport, y establezca su valor en True.
4. Reinicie la aplicación Citrix Workspace para que los cambios surtan efecto.

> **Nota:**
>
> Esto solo se aplica a las sesiones de Workspace (en la nube).

**Problemas conocidos:**

- En una configuración con varios monitores, las ventanas de aplicaciones en una sesión de escritorio de la aplicación Citrix Workspace se mueven a un monitor diferente. Este problema se produce cuando se desconecta de una sesión y se conecta a ella de nuevo.
- Esta función no está disponible en el inicio por explorador web.

Puede enviar comentarios sobre esta función a través del formulario de Podio.

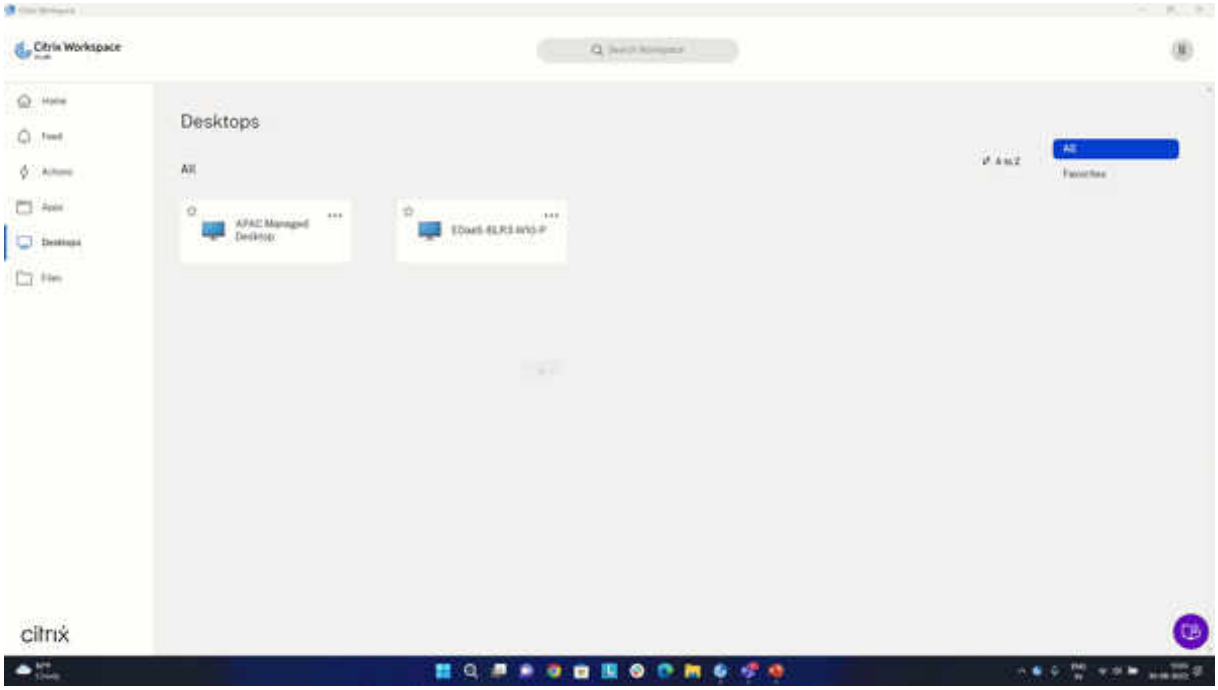
> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta

> en entornos de producción.

### Inicio rápido de escritorios desconectados [Technical Preview]

Al habilitar esta función, puede abrir al instante escritorios que estaban desconectados. Una vez habilitada esta función, la aplicación Citrix Workspace inicia las sesiones desconectadas en modo oculto. La sesión se presenta al instante en cuanto se abre el escritorio.




> **Nota:**
>
> Esto solo se aplica a las sesiones de Workspace (en la nube).

Puede registrarse para obtener esta versión Technical Preview a través del formulario de Podio.

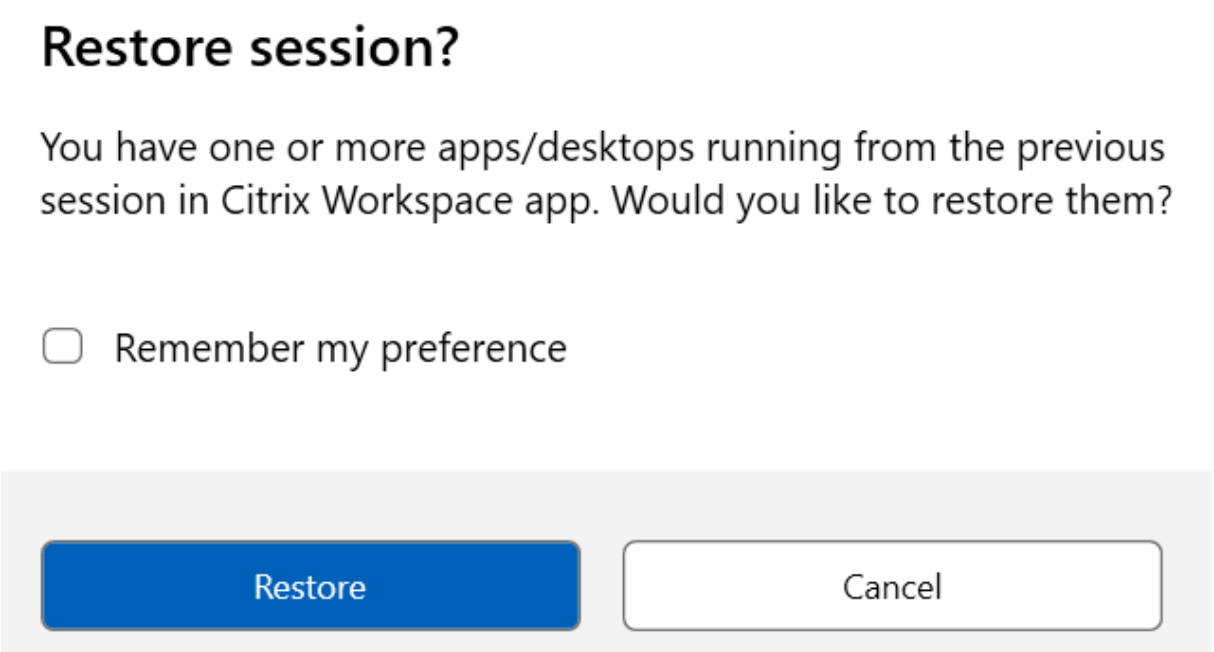
> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

### Experiencia mejorada al reconectar aplicaciones y escritorios virtuales

La versión 2302 de Citrix Workspace ofrece una experiencia de usuario mejorada al volver a conectarse a las aplicaciones y escritorios virtuales de los que se había desconectado.

Cuando la aplicación Citrix Workspace intenta actualizar la aplicación Citrix Workspace desconectada o iniciar nuevas aplicaciones o escritorios virtuales como parte de la funcionalidad de control del espacio de trabajo, aparece el siguiente mensaje:




Este mensaje solo aparece cuando la opción para **mostrar la solicitud de reconexión para volver a conectar las sesiones** se establece en “true” en Global App Configuration Service.

Haga clic en **Restaurar** para volver a conectarse y abrir las aplicaciones y escritorios virtuales nuevos y desconectados. Si solo quiere iniciar las aplicaciones y escritorios recién seleccionados, haga clic en **Cancelar**.

También puede seleccionar la opción **Recordar mi preferencia** para aplicar la preferencia seleccionada al siguiente inicio de sesión.

El mensaje **¿Restaurar sesión?** anterior aparecerá solo si:

- el usuario intenta iniciar una aplicación perteneciente a un almacén del espacio de trabajo;
- las directivas administrativas o los parámetros de configuración de la aplicación no están configurados para la funcionalidad de control del espacio de trabajo;
- las opciones de reconexión de control del espacio de trabajo están configuradas de forma predeterminada en el cliente.

> **Nota:**
>
> La configuración de reconexión de **Opciones de reconexión** tiene prioridad sobre las preferencias establecidas en el cuadro de diálogo. Para obtener más información, consulte Configurar opciones de reconexión mediante el cuadro de diálogo Preferencias avanzadas.

### Programa para la mejora de la experiencia del usuario (CEIP)

| Datos recopilados | Descripción | Para qué se utiliza |
|---|---|---|
| Datos de uso y configuración | El programa para la mejora de la experiencia del usuario de Citrix (Customer Experience Improvement Program o CEIP) recopila información de uso y configuración de la aplicación Citrix Workspace para Windows y envía esos datos automáticamente a Citrix y a Google Analytics. | Estos datos ayudan a Citrix a mejorar la calidad, la funcionalidad y el rendimiento de la aplicación Citrix Workspace, asignar adecuadamente los recursos para el desarrollo de productos, mantener los niveles de servicio y administrar la inversión en personal e infraestructura. |

#### Datos recopilados

Como se indicó anteriormente, Citrix recopila datos de uso y configuración de la aplicación Workspace para mejorar la calidad, la funcionalidad y el rendimiento de la aplicación Workspace, y para poder asignar adecuadamente los recursos para el desarrollo de productos, así como para mantener los niveles de servicio y administrar la inversión en personal e infraestructura. Los datos se utilizan y analizan únicamente de forma agregada. No se singulariza a ningún usuario o máquina ni se hacen análisis de usuarios finales específicos en función de los datos del CEIP.

Elementos concretos de datos CEIP recopilados por Google Analytics:

| | | | |
|---|---|---|---|
| Versión del sistema operativo* | Versión de la aplicación Workspace* | Configuración de la autenticación | Idioma de la aplicación Workspace |
| Método de inicio de sesiones | Error de conexión | Protocolo de conexión | Información de VDA |
| Configuración del instalador | Estado del instalador | Distribución del teclado del cliente | Configuración del almacén |
| Preferencia de actualización automática | Uso de la Central de conexiones | Configuración de protección de aplicaciones | Motivo de la pancarta sin conexión |

| | | | |
|---|---|---|---|
| Modelo/propiedades del dispositivo | Estado de inicio de las sesiones de Citrix Virtual Apps and Desktops | Nombre de escritorio/aplicación virtual | Estado de la actualización automática |
| Detalles de la concesión de conexiones | Uso de la función de migración de direcciones URL de StoreFront a Workspace | Uso de Citrix Enterprise Browser | Canal de actualización automática |
| Detalles del tiempo de espera por inactividad | Versión de Citrix Enterprise Browser | | |

> **Nota:**
>
> A partir de la versión 2206, la aplicación Citrix Workspace no recopila ningún dato de CEIP de los usuarios que se encuentran en la Unión Europea (UE), el Espacio Económico Europeo (EEE), Suiza y el Reino Unido (Reino Unido). Actualice la aplicación Workspace si quiere aprovechar esta funcionalidad.

**Preferencias para la recopilación de datos**

A partir de la versión 2205, tanto los usuarios como los administradores pueden dejar de enviar datos de CEIP (excepto los dos elementos de datos que se pueden bloquear como se especifica en la Nota a continuación) siguiendo estos pasos.

1. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace situado en el área de notificaciones.
2. Seleccione **Preferencias avanzadas**.
   Aparecerá el cuadro de diálogo **Preferencias avanzadas**.
3. Seleccione **Recopilación de datos**.
4. Seleccione **No, gracias** para inhabilitar CEIP o dejar de participar en el programa.
5. Haga clic en **Guardar**.

También puede ir a la siguiente entrada del Registro como administrador y establecer el valor como se sugiere:

**Ruta:** `HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

**Clave:** `Enable_CEIP`

**Valor:** `False`

> **Nota:**
>
> Una vez que haya seleccionado **No, gracias** o establecido la clave `Enable_CEIP` en `False`, también podrá dejar de enviar los dos últimos elementos de datos de CEIP, es decir, la versión de la aplicación Workspace y del sistema operativo, si va a la siguiente entrada del Registro y define el valor:

**Ruta**: `HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

**Clave**: `DisableHeartbeat`

**Valor**: `True`

#### Información adicional

Citrix gestiona sus datos de acuerdo con las condiciones de su contrato con Citrix y los protege como se especifica en el documento Citrix Services Security Exhibit. El documento Citrix Services Security Exhibit está disponible en el Centro de confianza de Citrix.

### Parámetros de región

La aplicación Citrix Workspace muestra la fecha, la hora y el número en función de la configuración regional del explorador web o del dispositivo de punto final.

A partir de la aplicación Citrix Workspace 2106, puede personalizar los formatos regionales de fecha, hora y número mediante los Parámetros regionales. Los cambios realizados en estos parámetros se guardan para un usuario individual y se aplican en todos los dispositivos.

> **Nota:**
>
> Esta opción solo está disponible en implementaciones de la nube.

Para obtener más información, consulte Configuración regional.

### Microsoft Teams

- Pantalla compartida
- Estimador de rendimiento del codificador
- Eliminación de eco acústico

#### Versión mejorada de WebRTC para Microsoft Teams optimizado

A partir de la versión 2209, la versión de WebRTC que se utiliza para Microsoft Teams optimizado se ha actualizado a la versión M98.

#### Efectos y desenfoque de fondo para la optimización de Microsoft Teams con HDX

Ahora, la aplicación Citrix Workspace para Windows admite efectos y el desenfoque de fondo en la optimización de Microsoft Teams con HDX.

Puede difuminar o reemplazar el fondo por una imagen personalizada y evitar distracciones inesperadas al ayudar a que la conversación se centre en la silueta (cuerpo y rostro). La función se puede utilizar con llamadas de conferencia o entre dos usuarios.

> **Nota:**
>
> Ahora, esta función está integrada en los botones y la interfaz de usuario de Microsoft Teams. La compatibilidad con varias ventanas es un requisito previo que necesita una actualización de VDA a la versión 2112 o a una posterior. Para obtener más información, consulte Reuniones y chat en modo multiventana.

**Limitaciones:**

- No se admite el reemplazo de fondo definido por el administrador y el usuario.
- El efecto de fondo no persiste entre sesiones. Cuando cierra y reinicia Microsoft Teams o el VDA se conecta de nuevo, el efecto de fondo se restablece y se desactiva.
- Cuando la sesión ICA se conecta de nuevo, el efecto está desactivado. Sin embargo, la interfaz de usuario de Microsoft Teams muestra que el efecto anterior sigue activado con una marca de verificación. Citrix y Microsoft están trabajando juntos para resolver este problema.
- El dispositivo debe estar conectado a Internet mientras se reemplaza la imagen de fondo.

> **Nota:**
>
> Esta función estará disponible solamente después de la implantación de una futura actualización de Microsoft Teams. Cuando Microsoft implante la actualización, puede consultar CTX253754 y el Plan de desarrollo público de Microsoft 365 para obtener información sobre el anuncio y la actualización de la documentación.

#### Pantalla compartida

A partir de la versión 2006.1, hay nuevas funcionalidades en la función saliente de uso compartido de la pantalla para la aplicación Microsoft Teams que emplea la optimización HDX.

El contenido compartido con Microsoft Teams se limita al contenido de la ventana de **Desktop Viewer**. Todo lo que está fuera de la ventana de **Desktop Viewer** (escritorio local del cliente, aplicaciones) se oscurece.

En un sistema operativo Windows 10, los siguientes elementos no se oscurecen cuando se superponen a la ventana de **Desktop Viewer**:

- El menú Inicio, el menú Buscar y la vista de tareas.

- La barra de notificaciones y las notificaciones que aparecen en el lado derecho de la barra de tareas.
- En una configuración de varios monitores con diferentes parámetros de PPP, si una aplicación local se superpone a dos monitores diferentes y su cantidad de PPP no coincide con la del monitor principal que tiene la ventana de Desktop Viewer.
- La aplicación y la vista previa que se muestran al pasar el mouse sobre el icono de la aplicación en la barra de tareas.

#### Estimador de rendimiento del codificador

`HdxRtcEngine.exe` es el motor de medios WebRTC integrado en la aplicación Citrix Workspace que gestiona la redirección de Microsoft Teams. A partir de la aplicación Citrix Workspace 1912 o una versión posterior, `HdxRtcEngine.exe` puede estimar la mejor resolución de codificación que la CPU del dispositivo de punto final puede soportar sin sobrecargarse. Los valores posibles son: 240p, 360p, 480p, 720p y 1080p.

El proceso de estimación del rendimiento (también llamado `webrtcapi.EndpointPerformance`) se ejecuta cuando se inicializa HdxTeams.exe. El código de macrobloque determina la mejor resolución que se puede lograr en ese dispositivo de punto final en cuestión. La negociación del códec incluye la resolución más alta posible. La negociación del códec puede ser entre los pares o entre el par y el servidor de conferencias.

Existen cuatro categorías de rendimiento para los dispositivos de punto final que tienen su propia resolución **máxima** disponible:

| Rendimiento del dispositivo de punto final | Resolución máxima | Valor de clave del Registro |
|---|---|---|
| rápido | 1080p (1920x1080 16:9 @ 30 fps) | 3 |
| medio | 720p (1280x720 16:9 @ 30 fps) | 2 |
| lento | 360p (640x360 16:9 @ 30 fps o 640x480 4:3 @ 30 fps) | 1 |
| muy lento | 240p (320x180 16:9 @ 30 fps o 320x240 4:3 @ 30 fps) | 0 |

#### Ruta al Registro en la aplicación Citrix Workspace:

Vaya a la ruta del Registro HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream y cree esta clave:

| Name | Tipo | Valores | Descripción |
|---|---|---|---|
| OverridePerformance | DWORD | 0;1;2;3 | Fuerza el rendimiento deseado. El valor debe estar en el intervalo entre 0 y 3, donde 0 indica lento, y 3, rápido. |

Para obtener información sobre cómo configurar el codificador de dispositivos de punto final, consulte Estimador de rendimiento del codificador.

Para obtener más información sobre la optimización de Microsoft Teams, consulte Optimización para Microsoft Teams.

#### Eliminación de eco acústico

La eliminación del eco en `HdxRtcEngine.exe` puede inhabilitarse para solucionar problemas de rendimiento de audio o de compatibilidad con periféricos que tienen prestaciones de AEC integradas.

Vaya a la ruta del Registro HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream y cree esta clave:

Nombre: EnableAEC
Tipo: REG_DWORD
Datos: 0
(0 inhabilita AEC y 1 habilita AEC; si `Regkey` no está presente, el comportamiento predeterminado en HdxRtcEngine es el de habilitar AEC, independientemente de las prestaciones de hardware del periférico).

#### Mejoras en la optimización de Microsoft Teams

- A partir de la aplicación Citrix Workspace 2112.1 para Windows, estas funciones (Multiventana y Dar/Tomar el control) solo están disponibles después de la implantación de actualizaciones futuras de Microsoft Teams.

  Cuando Microsoft implante la actualización, consulte CTX253754 para obtener información sobre la actualización de la documentación y el anuncio.

  - **Reuniones y chats en varias ventanas para Microsoft Teams**: Puede usar varias ventanas para chats y reuniones en Microsoft Teams cuando HDX lo optimiza en Citrix Virtual Apps and Desktops (2112 o una versión posterior). Puede separar las conversaciones o

las reuniones de varias maneras. Para obtener detalles sobre la función de ventana emergente, consulte Teams Pop-Out Windows for Chats and Meetings en el sitio de Microsoft Office 365.

Si ejecuta una versión anterior de la aplicación Citrix Workspace o Virtual Delivery Agent (VDA), es posible que Microsoft retire el código de las ventanas únicas en el futuro. Sin embargo, puede actualizarlos a la versión de VDA o de la aplicación Citrix Workspace que admita varias ventanas (2112 y versiones posteriores) antes de que hayan transcurrido nueve meses de la fecha en que la función se puso a disposición general.

- **Dar control**: Puede usar el botón **Dar control** para otorgar el control de su pantalla compartida a otros usuarios que participan en la reunión. El otro participante puede seleccionar elementos y modificar la pantalla compartida mediante el teclado, el mouse y el portapapeles. Los dos tendrán el control de la pantalla compartida y usted podrá recuperar el control en cualquier momento.
- **Solicitar control**: Durante las sesiones de uso compartido de pantalla, cualquier participante puede solicitar el control a través del botón **Solicitar control**. La persona que comparte la pantalla puede aprobar o rechazar la solicitud. Cuando tiene el control, puede controlar el teclado y el mouse en la pantalla compartida y liberar el control para dejar de compartir el control.

**Limitación:**

La opción **Solicitar el control** no está disponible durante llamadas entre un usuario optimizado y un usuario en el cliente de escritorio de Microsoft Teams nativo en el dispositivo de punto final. Como solución temporal, los usuarios pueden unirse a una reunión para obtener la opción **Solicitar el control**.

- **E911 dinámico**: La aplicación Citrix Workspace admite llamadas de emergencia dinámicas. Cuando se usa en los planes de llamadas de Microsoft, Operator Connect y enrutamiento directo, proporciona la opción de:
  - configurar y redirigir llamadas de emergencia
  - notificar al personal de seguridad

  La notificación se envía en función de la ubicación actual de la aplicación Citrix Workspace que se ejecuta en el dispositivo de punto final, en lugar del cliente de Microsoft Teams del VDA.
  La ley de Ray Baum exige que la ubicación transmitible de la persona que llama al 911 se transmita al Punto de Respuesta de Seguridad Pública (PSAP) correspondiente. A partir de la aplicación Citrix Workspace 2112.1 para Windows, la optimización para Microsoft Teams con HDX cumple con la ley de Ray Baum.
- **Uso compartido de aplicaciones**: Antes no podía compartir aplicaciones mediante la función **Compartir pantalla** en Microsoft Teams al habilitar la directiva HDX 3D Pro en Citrix

Studio.

A partir de la aplicación Citrix Workspace 2112.1 para Windows y Citrix Virtual Apps and Desktops 2112, la función de **uso compartido de la pantalla** le permite compartir aplicaciones en Microsoft Teams. Puede compartir aplicaciones cuando la directiva de HDX 3D Pro esté habilitada.

- A partir de la aplicación Citrix Workspace 2109.1 para Windows, están disponibles las siguientes funciones:
  - **Compatibilidad con WebRTC 1.0**: La aplicación Citrix Workspace 2109.1 para Windows admite WebRTC 1.0 para ofrecer una mejor experiencia en videoconferencias junto en la vista de galería.
  - **Mejora del uso compartido de la pantalla**: Puede compartir aplicaciones individuales, ventanas o la pantalla completa mediante la función de uso compartido de la pantalla en Microsoft Teams. Citrix Virtual Delivery Agent 2109 es un requisito previo para esta función.
  - **Compatibilidad con la protección de aplicaciones**: Ahora, cuando la protección de aplicaciones está habilitada, puede compartir contenido a través de Microsoft Teams con la optimización de HDX. Con esta función, puede compartir la ventana de aplicaciones que se ejecutan en el escritorio virtual. Citrix Virtual Delivery Agent 2109 es un requisito previo para esta función.

  > **Nota:**
  >
  > El uso compartido total del escritorio o de los monitores se inhabilita cuando la protección de aplicaciones se habilita para el grupo de entrega.

- La aplicación Citrix Workspace 2109.1 para Windows admite lo siguiente en Microsoft Teams optimizado de aplicaciones alojadas por VM:
  - Llamadas de audio y vídeo entre dos usuarios
  - Llamada de conferencias
  - Pantalla compartida
- A partir de la aplicación Citrix Workspace 2106 para Windows:
  - Cuando Desktop Viewer se halla en modo de pantalla completa, el usuario puede seleccionar una de todas las pantallas que cubren Desktop Viewer para compartirla. En el modo de ventana, el usuario puede compartir la ventana de Desktop Viewer. En el modo integrado, el usuario puede seleccionar una de todas las pantallas para compartirla. Cuando Desktop Viewer cambia el modo de ventana (maximizada, restaurada o minimizada), la pantalla compartida se detiene.
- A partir de la aplicación Citrix Workspace 2105 para Windows:
  - Puede configurar una interfaz de red preferida para el tráfico multimedia.

Vaya a `\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream` y cree una clave llamada `NetworkPreference`(REG_DWORD).

Seleccione uno de estos valores según corresponda:

* 1: Ethernet
* 2: Wi-Fi
* 3: Móvil
* 5: Bucle invertido
* 6: Cualquiera

De forma predeterminada y si no se establece ningún valor, el motor de medios WebRTC elige la mejor ruta disponible.

- Puede inhabilitar el módulo del dispositivo de audio 2 (ADM2) para que el módulo de dispositivo de audio (ADM) heredado se utilice para micrófonos de cuatro canales. Inhabilitar ADM2 ayuda a resolver problemas relacionados con los micrófonos en las llamadas.

  Para inhabilitar ADM2, vaya a `\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`, cree una clave denominada `DisableADM2` (REG_DWORD) y establezca el valor en `1`.

- A partir de la aplicación Citrix Workspace 2103.1 para Windows:
  - Ahora el códec de vídeo VP9 está inhabilitado de forma predeterminada.
  - Mejora en la eliminación de eco, el control automático de ganancias y configuraciones de supresión de ruido: Si Microsoft Teams configura estas opciones, la instancia de Microsoft Teams redirigida por Citrix respeta los valores tal y como están configurados. De lo contrario, estas opciones se establecen en **True** de forma predeterminada.
  - Ahora `DirectShow` es el generador predeterminado.

    **Para cambiar el generador predeterminado, haga esto:**

    1. Abra el Editor del Registro.
    2. Vaya a esta ubicación de clave: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`.
    3. Actualice este valor: `"UseDirectShowRendererAsPrimary"=dword:00000000`

       Otros valores posibles:

       * 0: Media Foundation
       * 1: DirectShow (predeterminado)

    4. Vuelva a iniciar la aplicación Citrix Workspace.

- A partir de la aplicación Citrix Workspace 2012 para Windows:
  - Ahora, los usuarios pueden ver el puntero del presentador en una sesión de pantalla compartida.

  - El motor de medios WebRTC ahora tiene en cuenta el servidor proxy configurado en el dispositivo cliente.

- A partir de la aplicación Citrix Workspace 2009.6 para Windows:
  - Microsoft Teams muestra los dispositivos periféricos utilizados anteriormente en la lista **Dispositivos preferidos**.
  - El motor de medios WebRTC determina con precisión la resolución máxima de codificación posible en un dispositivo de punto final. El motor de medios WebRTC realiza estimaciones varias veces al día y no solo al iniciarse por primera vez.
  - El instalador de la aplicación Citrix Workspace incluye tonos de llamada de Microsoft Teams.
  - Mejoras en la eliminación del eco: Se ha reducido el nivel de eco cuando un compañero tiene un altavoz o un micrófono que generan eco.
  - Mejoras en el uso compartido de la pantalla: Al compartir la pantalla, solo la pantalla de **Desktop Viewer** se captura en formato de mapa de bits nativo. Antes, las ventanas locales del cliente que quedaban se superponían a la ventana de **Desktop Viewer** quedaban oscurecidas.

- A partir de la aplicación Citrix Workspace 2002 para Windows:
  - Cuando comparte el espacio de trabajo mediante Microsoft Teams, la aplicación Citrix Workspace muestra un borde rojo que rodea el área del monitor que se está compartiendo. Solo se puede compartir la ventana de **Desktop Viewer** o cualquier ventana local superpuesta encima de este. Cuando se minimiza la ventana de **Desktop Viewer**, el uso compartido de pantalla se pausa.

- A partir de la aplicación Citrix Workspace 2302 para Windows:
  - **Se ha actualizado el modo de seleccionar dispositivos de audio para Microsoft Teams optimizado**: Al cambiar los dispositivos de audio predeterminados en la configuración de sonido del dispositivo de punto final, Microsoft Teams optimizado en la imagen de disco virtual (VDI) de Citrix VDI cambia la selección actual de dispositivos de audio para que coincida con los valores predeterminados del dispositivo de punto final.

    Sin embargo, si selecciona un dispositivo de forma explícita en Microsoft Teams, su selección tendrá prioridad y no seguirá los valores predeterminados del dispositivo de punto final. Su selección se mantendrá hasta que borre la memoria caché de Microsoft Teams.

- A partir de la aplicación Citrix Workspace 2303 para Windows:
  - Experiencia mejorada para llamadas de videoconferencia de Microsoft Teams optimizado: La función de transmisión simultánea está habilitada de forma predeterminada para las llamadas de videoconferencia de Microsoft Teams optimizado. Con esta compatibilidad, la calidad y la experiencia de las videoconferencias en diferentes dispositivos de punto

final mejoran al adaptarse a la resolución adecuada para ofrecer la mejor experiencia en llamadas a todos los usuarios.

Con esta experiencia mejorada, es posible que cada usuario cuente con varias transmisiones de vídeo en diferentes resoluciones (por ejemplo, 720p, 360p…) en función de varios factores, como la capacidad del dispositivo de punto final, las condiciones de la red y más. El dispositivo de punto final receptor solicita entonces la resolución de máxima calidad que pueda gestionar, lo que ofrece a todos los usuarios una experiencia de vídeo óptima.

> **Nota:**
>
> Esta función está disponible solamente después de la implantación de una actualización de Microsoft Teams. Para obtener información sobre ETA, vaya a y busque la hoja de ruta de Microsoft 365. Cuando Microsoft implante la actualización, consulte CTX253754 para obtener información sobre la actualización de la documentación y el anuncio.

## Configurar Single Sign-On en la aplicación Workspace

April 6, 2023

### Single Sign-On mediante Azure Active Directory

En esta sección se explica cómo implementar Single Sign-On (SSO) con Azure Active Directory (AAD) como proveedor de identidades con cargas de trabajo unidas a un dominio en dispositivos de punto final híbridos o inscritos en AAD. Con esta configuración, puede autenticarse en Workspace mediante Windows Hello o FIDO2 en dispositivos de punto final que están inscritos en AAD.

> **Nota:**
>
> Si usa Windows Hello como autenticación independiente, puede usar Single Sign-On en la aplicación Citrix Workspace, pero se le solicitará el nombre de usuario y la contraseña al acceder a aplicaciones o escritorios virtuales publicados. Como solución temporal, considere la posibilidad de implementar el Servicio de autenticación federada (FAS).

#### Requisitos previos

- Una conexión activa de Azure Active Directory a Citrix Cloud. Para obtener más información, consulte Conectar Azure Active Directory a Citrix Cloud.
- Una autenticación del espacio de trabajo de Azure Active Directory. Para obtener más información, consulte Habilitar la autenticación de Azure AD para espacios de trabajo.

- Compruebe si configuró Azure AD Connect. Para obtener más información, consulte Introducción a Azure AD Connect mediante la configuración rápida.
- Active la autenticación PassThrough en Azure AD Connect. Igualmente, verifique si las opciones de Single Sign-On y PassThrough funcionan en Azure Portal. Para obtener más información, consulte Autenticación de paso a través de Azure Active Directory: Guía de inicio rápido.

#### Configuración

Siga estos pasos para configurar SSO en su dispositivo:

1. Instale la aplicación Citrix Workspace mediante la línea de comandos de Windows con la opción `includeSSON`:

```
CitrixWorkspaceApp.exe /includeSSON
```

1. Reinicie el dispositivo.
2. Ejecute `gpedit.msc` para abrir la plantilla administrativa de GPO de la aplicación Citrix Workspace.
3. Vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Autenticación de usuarios** > **Nombre de usuario y contraseña locales**.
4. Seleccione **Habilitar autenticación PassThrough**. En función de la configuración y los parámetros de seguridad, seleccione la opción **Permitir autenticación PassThrough para todas las conexiones ICA** para que la autenticación PassThrough funcione.
5. Modifique los parámetros de Autenticación del usuario en Internet Explorer. Para modificar los parámetros:
   - Abra **Propiedades de Internet** en el Panel de control.
   - Vaya a **Propiedades generales** > **Intranet local** y haga clic en **Sitios**.
   - En la ventana **Intranet local**, haga clic en **Opciones avanzadas > Agregar este sitio a la zona de:**, agregue estos sitios de confianza y haga clic en **Cerrar**:
     - `https://aadg.windows.net.nsatc.net`
     - `https://autologon.microsoftazuread-sso.com`
     - `The name of your tenant, for example: https://xxxtenantxxx.cloud.com`
6. Para inhabilitar las solicitudes de autenticación adicionales, inhabilite el atributo `prompt=login` en su arrendatario. Para obtener más información, consulte User Prompted for Additional Credentials on Workspace URLs When Using Federated Authentication Providers. Puede ponerse en contacto con la asistencia técnica de Citrix para inhabilitar el atributo `prompt=login` en su arrendatario y configurar correctamente Single Sign-On.

7. Habilite la autenticación PassThrough de dominio en el cliente de la aplicación Citrix Workspace. Para obtener más información, consulte Autenticación PassThrough de dominio.
8. Reinicie la aplicación Citrix Workspace para que los cambios surtan efecto.

### Single Sign-On mediante Okta y el Servicio de autenticación federada

En esta sección se explica cómo puede implementar Single Sign-On (SSO) mediante Okta como proveedor de identidades con un dispositivo unido a un dominio y el Servicio de autenticación federada (FAS). Con esta configuración, puede autenticarse en Workspace mediante Okta para habilitar Single Sign-On y evitar que se solicite un segundo inicio de sesión. Para que este mecanismo de autenticación funcione, debe usar el Servicio de autenticación federada de Citrix con Citrix Cloud. Para obtener más información, consulte Conectar el Servicio de autenticación federada de Citrix con Citrix Cloud.

#### Requisitos previos

- Cloud Connector. Para obtener más información sobre la instalación de Cloud Connector, consulte Instalar Cloud Connector.
- Un agente de Okta. Para obtener más información sobre la instalación de un agente de Okta, consulte Install the Okta Active Directory agent. Además, puede configurar el agente web de Okta IWA para que inicie sesión desde un dispositivo unido a un dominio de Windows. Para obtener más información, consulte Install and configure the Okta IWA Web agent for Desktop single sign-on.
- Una conexión activa de Azure Active Directory a Citrix Cloud. Para obtener más información, consulte Conectar Azure Active Directory a Citrix Cloud.
- Servicio de autenticación federada. Para obtener más información, consulte Instalar el Servicio de autenticación federada.

#### Configuración

Siga estos pasos para configurar SSO en su dispositivo:

**Conecte Citrix Cloud con su organización de Okta**:

1. Descargue e instale el agente de Active Directory para Okta. Para obtener más información, consulte Install the Okta Active Directory agent.
2. Inicie sesión en Citrix Cloud desde `https://citrix.cloud.com`.
3. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.

4. Busque Okta y seleccione **Conectar** en el menú de tres puntos.
5. En **URL de Okta**, introduzca su dominio de Okta.
6. En **Token de API de Okta**, introduzca el token de API de su organización de Okta.
7. En **ID de cliente** y **Secreto del cliente**, introduzca el ID y el secreto del cliente de la integración de la aplicación web OIDC que creó antes. Para copiar estos valores de la consola de Okta, seleccione **Aplicaciones** y busque su aplicación de Okta. En **Credenciales del cliente**, utilice el botón **Copiar al portapapeles** para cada valor.
8. Haga clic en **Probar y finalizar**. Citrix Cloud verifica los detalles de Okta y prueba la conexión.

**Habilite la autenticación con Okta para espacios de trabajo**:

1. En el menú de Citrix Cloud, seleccione **Configuración de Workspace** > **Autenticación**.
2. Seleccione **Okta**. Cuando se le solicite, seleccione **Comprendo los efectos en la experiencia de uso de los suscriptores**.
3. Haga clic en **Aceptar** para aceptar la solicitud de permisos.

**Habilite el Servicio de autenticación federada**.

1. En el menú de Citrix Cloud, seleccione **Configuración de Workspace** y, luego, **Autenticación**.
2. Haga clic en **Habilitar FAS**. Este cambio puede tardar hasta cinco minutos en aplicarse a las sesiones de los suscriptores.

Posteriormente, el Servicio de autenticación federada (FAS) se activa para todos los inicios de aplicaciones virtuales y escritorios de Citrix Workspace.

Cuando los suscriptores inician sesión en su espacio de trabajo e inician una aplicación virtual o un escritorio en la misma ubicación de recursos que el servidor FAS, la aplicación o el escritorio se inician sin solicitar credenciales.

> **Nota:**
>
> Si todos los servidores de FAS de una ubicación de recursos están inactivos o están en modo de mantenimiento, los inicios de aplicación se ejecutan correctamente, pero Single Sign-On no está activo. Se solicita a los suscriptores sus credenciales de AD para acceder a cada aplicación o escritorio.

## Administración de aplicaciones cliente

March 31, 2023

La aplicación Citrix Workspace para Windows ofrece funcionalidad de administración de aplicaciones cliente, lo que la convierte en la única aplicación cliente necesaria en el dispositivo de punto final para instalar y administrar agentes, como el agente de Secure Access y el plug-in End Point Analysis (EPA).

Con esta capacidad, los administradores pueden implementar y administrar fácilmente los agentes necesarios desde una única consola de administración.

> **Nota:**
>
> Esta funcionalidad solo es aplicable a las sesiones de Workspace (en la nube).

La administración de aplicaciones cliente incluye los siguientes pasos:

- Los administradores deben especificar los agentes necesarios en los dispositivos de los usuarios finales en Global App Configuration Service. Los administradores pueden especificar el agente de Secure Access y el agente de Endpoint Analysis (EPA).
- La aplicación Citrix Workspace obtiene la lista de agentes de Global App Configuration Service.
- Según la lista obtenida de Global App Configuration Service, la aplicación Citrix Workspace descarga los paquetes de agente a través del servicio de actualización automática. Si el agente no se ha instalado anteriormente en el dispositivo de punto final, la aplicación Citrix Workspace desencadena la instalación del agente. Si el agente ya está instalado, la aplicación Citrix Workspace desencadena una actualización del agente (si la versión del agente descargado es posterior a la versión instalada).

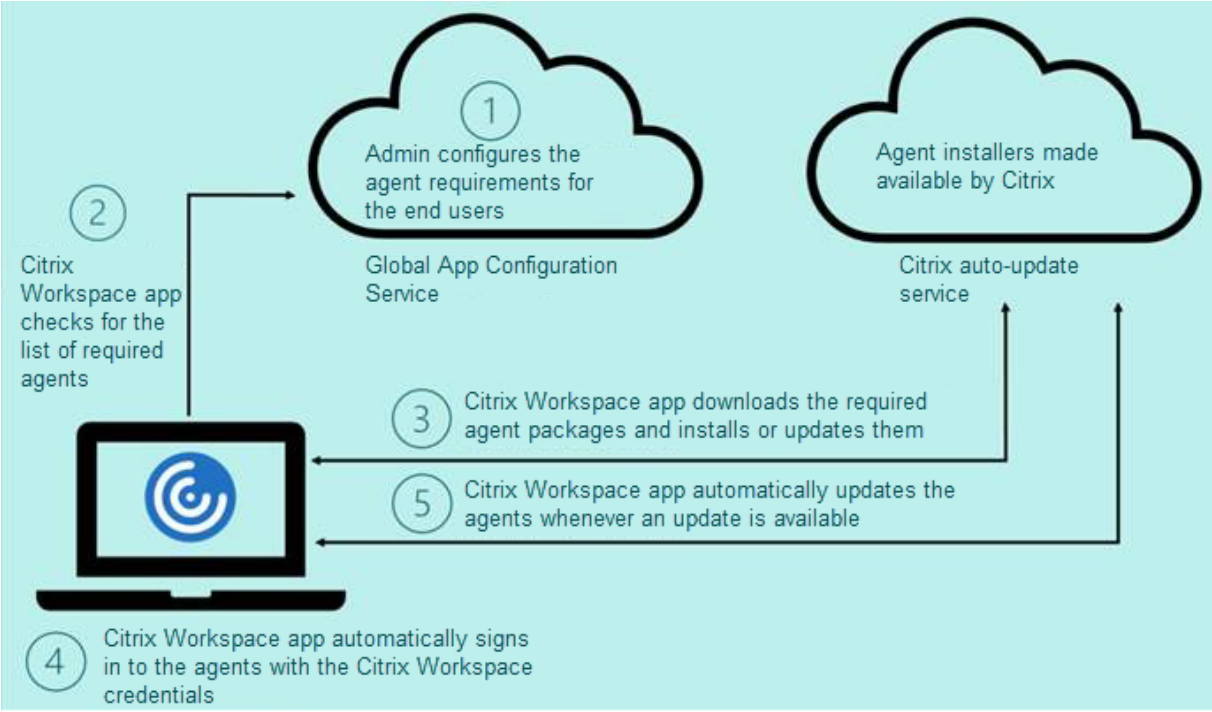
La aplicación Citrix Workspace garantiza la actualización automática de los agentes siempre que haya una actualización disponible en el futuro.

La aplicación Citrix Workspace inicia sesión automáticamente en los agentes con las credenciales de Citrix Workspace.

> **Notas:**
>
> - Si los plug-ins de EPA y ZTNA no existen, se descargan y se instalan al agregar el almacén o la cuenta por primera vez.
> - Si el almacén o la cuenta y los plug-ins ya existen y el instalador contiene una versión posterior, los plug-ins se actualizan durante el ciclo de actualización automática.

El siguiente diagrama ilustra el flujo de trabajo:




> **Importante**:
>
> Se requiere Global App Configuration Service para habilitar la función de administración de aplicaciones cliente.
>
> - Para los almacenes de la nube, se puede acceder a la interfaz de usuario de Global App Configuration Service en la sección **Configuración de Workspace** del portal de administración de Citrix Cloud.
> - Para incorporar almacenes locales o si los clientes necesitan configurar la detección por correo electrónico para los almacenes de la nube, consulte la documentación de Global App Configuration Service.

Puede habilitar la función de administración de aplicaciones cliente con estos métodos:

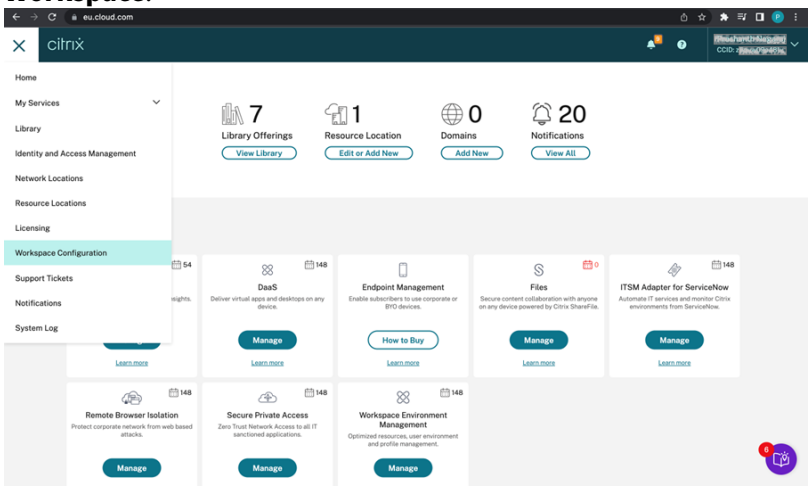
- Usar la interfaz de usuario de Global App Configuration Service: Use este método para implementar la versión más reciente del cliente.
- Usar la API de Global App Configuration Service: Use este método para personalizar la instalación mediante parámetros con el fin de controlar la versión, los modos de implementación, los intervalos de actualización automática…

### Habilitar la administración de aplicaciones cliente mediante la interfaz de usuario de Global App Configuration Service

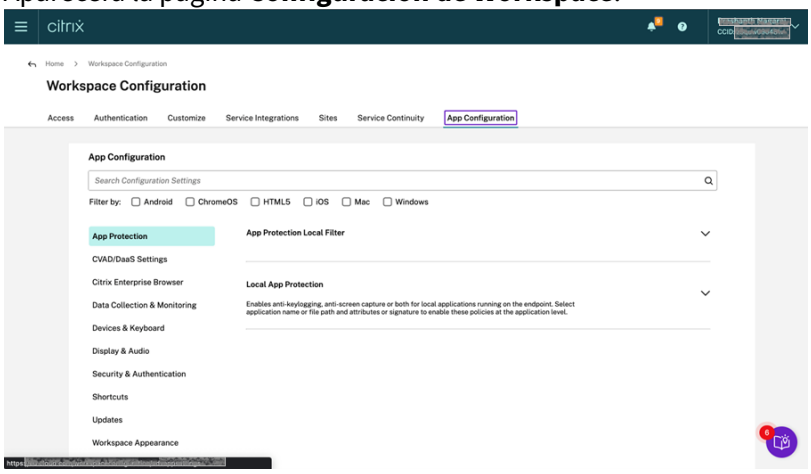
Este método solo se aplica a los almacenes de la nube. Los administradores pueden implementar agentes (EPA/Secure Access, Zoom o WebEx) mediante la interfaz de usuario.

1. Inicie sesión en Citrix Cloud.
2. En el menú de la parte superior izquierda de la pantalla, seleccione **Configuración de Workspace**.

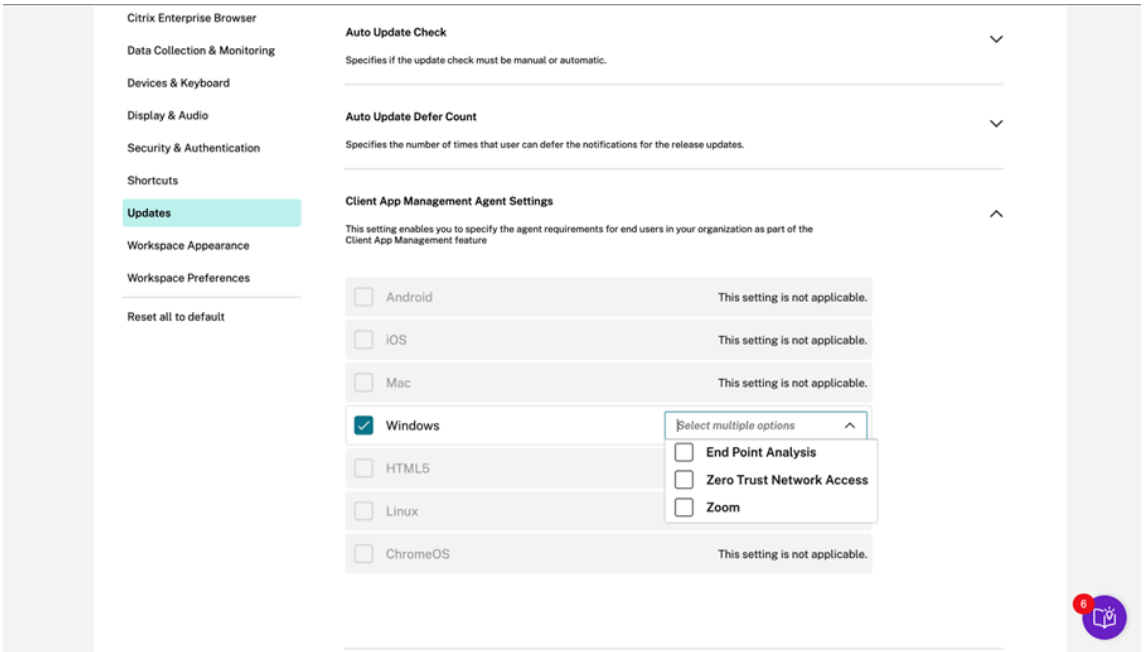



Aparecerá la página **Configuración de Workspace**.




3. Haga clic en la ficha **Configuración de aplicaciones**.
4. Haga clic en **Actualizaciones**.
5. Asegúrese de que la casilla **Windows** esté marcada.
6. Seleccione los agentes necesarios junto a **Windows** en la lista desplegable de **Parámetros del agente de administración de aplicaciones cliente**.




### Habilitar la administración de aplicaciones cliente mediante la API de Global App Configuration Service

1. Configure e incorpore los parámetros a Global App Configuration Service mediante la API. Para obtener más información, consulte Map service URLs and configure settings.
2. Se deben incorporar estos parámetros de Global App Configuration para que el almacén o la cuenta puedan incorporar EPA y los clientes ZTNA/Secure Access Client:

```
{

  "serviceURL": {

    "url": "https://storefront.acme.com:443"
   }
 ,
  "settings": {

    "name": "Install and update plugins",
    "description": "Install and update plugins",
    "useForAppConfig": true,
    "appSettings": {

      "windows": [{

        "AutoUpdate": {

```

```
          "AutoUpdatePluginsSettings": [{

              "pluginId": "8A8AF6C0-11F6-4343-BA2D-A85A766170D4",
              "pluginName": "Citrix EPA Client",
              "pluginSettings": {

                "isFTU": true,
                "isBlocking": true,
                "delayGroup": "Fast",
                "deploymentMode": "InstallAndUpdate",
                "detectRule": "UpgradeCode:{
37A181F7-870E-4BDF-B0EA-E3B4766119FE }
",
                "maximumAllowedVersion": "22.10.1.9",
                "minimumAllowedVersion": "0.0.0.0",
                "stream": "Current",
                "upgradeToLatest": true
               }

             }
,
            {

              "pluginId": "9A8AF6C0-11F6-4343-BA2D-A85A766170D5",
              "pluginName": "Citrix Secure Access Client",
              "pluginSettings": {

                "isFTU": true,
                "isBlocking": false,
                "delayGroup": "Fast",
                "deploymentMode": "InstallAndUpdate",
                "detectRule": "UpgradeCode:{
F0ED53AB-11BE-4E9C-87E5-CD4A81DA2A4D }
",
                "maximumAllowedVersion": "22.10.1.9",
                "minimumAllowedVersion": "0.0.0.0",
                "stream": "Current",
                "upgradeToLatest": true
               }

             }

          ],
          "userOverride": false
         }
```

```
64
65          }
66   ]
67        }
68
69     }
70
71   }
72
73
74
75 <!--NeedCopy-->
```

Esta tabla muestra el esquema, los valores y la descripción de los parámetros de la administración de aplicaciones cliente.

|Parámetro del esquema|Valor| Descripción|
|—|—|—|
|isBlocking| True o False |Cuando el parámetro isBlocking se establece en true, el plug-in se considera obligatorio y la página de inicio de sesión solo aparece cuando está instalado el plug-in requerido. Citrix recomienda configurar EPA como plug-in obligatorio.|
|pluginName||Nombre descriptivo del plug-in. pluginName se puede modificar.|
|pluginId| |ID del plug-in y no debe modificarse.|
|delayGroup| Fast, Medium, Slow|
Intervalo de actualización automática en que los plug-ins deben actualizarse.|
|deploymentMode|InstallAndUpdate/Update|InstallAndUpdate: El plug-in puede instalarse de nuevo y actualizarse con la nueva versión. Novedad: Solo deben permitirse actualizaciones, no nuevas instalaciones. |
|None||No se necesita hacer nada para este plug-in.|
|detectRule|El valor no debe modificarse.| Comprueba si el plug-in ya está instalado o no.|
|maximumAllowedVersion| |La versión máxima permitida del plug-in.|
|minimumAllowedVersion| |La versión mínima permitida del plug-in.|
|upgradeToLatest|True o False|
Debe establecerse en false para poder usar maximumAllowedVersion y minimumAllowedVersion. True: La versión más reciente del plug-in es la que se tiene en cuenta durante la actualización.|
|Stream|Current|Debe establecerse en Current para recibir la instalación o la actualización automática de los plug-ins|

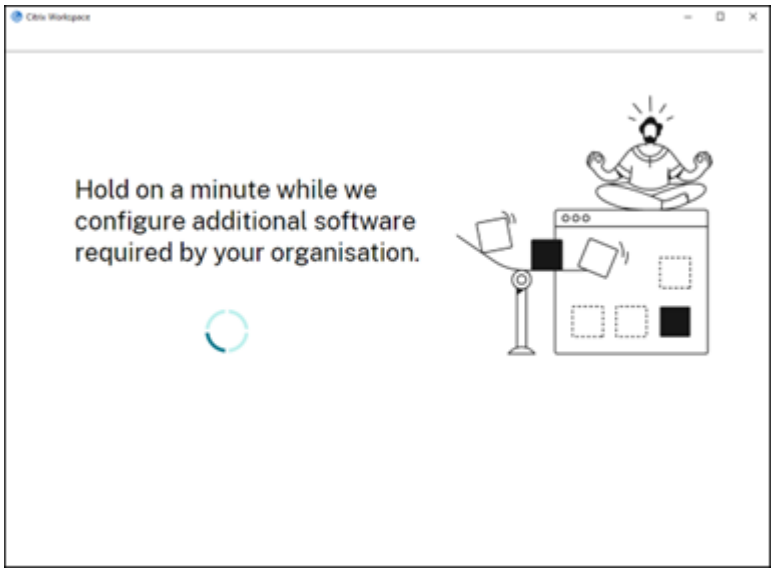
### Flujo de trabajo de los usuarios

1. Descargue e instale la aplicación Citrix Workspace para Windows, versión 2212.

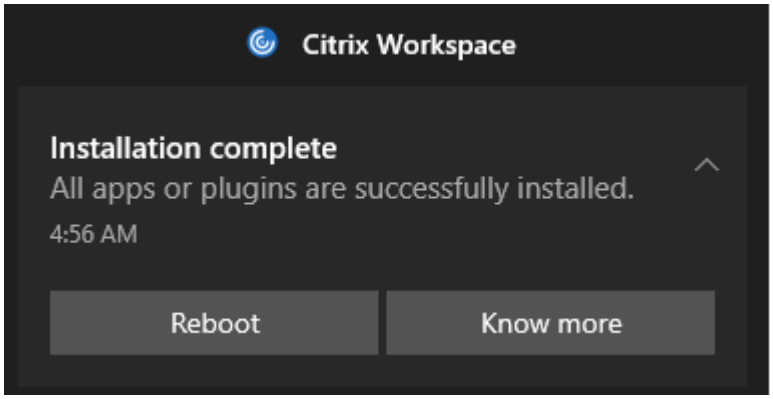
 

2. Haga clic en **Agregar cuenta** al terminar la instalación.
3. Agregue el almacén/cuenta donde están incorporados los ajustes de configuración de la aplicación.

   Al instalar los plug-ins obligatorios, aparece el siguiente mensaje:

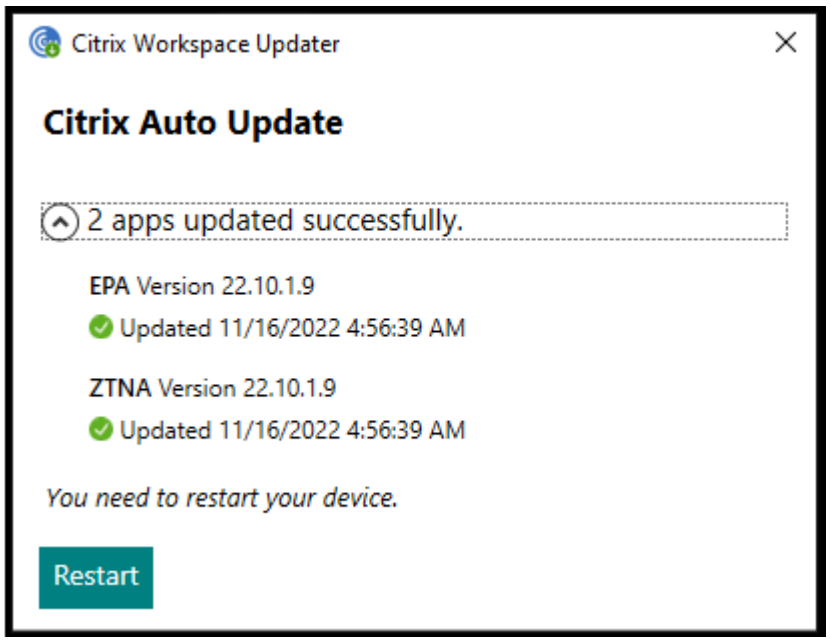



4. Cuando se complete la instalación, aparecerá esta notificación:




5. Haga clic en **Know More** para saber qué plug-ins hay instalados.




### Administración de aplicaciones de cliente para el plug-in Zoom

La descarga, la instalación y la actualización automática del plug-in Zoom también se admiten y se gestionan de la misma manera que los plug-ins de EPA y ZTNA.

> **Nota:**
>
> Esta funcionalidad solo es aplicable a las sesiones de Workspace (en la nube).

Para usar esta funcionalidad, se deben incorporar los siguientes ajustes de Global App Configuration para el almacén o cuenta:

```
{

  "serviceURL": {

    "url": "https://storefront.acme.com:443"

   }
 ,
  "settings": {

    "name": "Install and update plugins",

```

```
    "description": "Install and update plugins",

    "useForAppConfig": true,

    "appSettings": {


      "windows": [{


        "AutoUpdate": {


          "AutoUpdatePluginsSettings": [{


                  "pluginSettings": {


                    "upgradeToLatest": true,

                    "deployment Mode": "InstallAndUpdate",

                    "stream": "Current",

                    "isFTU": false,

                    "isBlocking": false,

                    "detectRule": "UpgradeCode:{
34225638-14F3-4059-BE34-175AC9B35435 }
",

                    "maximumAllowedVersion": "5.11.2872",

                    "minimumAllowedVersion": "0.0.0",

                    "delayGroup": "Fast"

                   }
,

                  "pluginName": "Zoom VDI AutoUpgrade Plugin",

                  "pluginId": "1A4BB471-022C-4C87-BDCD-0B64FB42869C"
```

```
62
63                      }
64                ],
65
66              "userOverride": false
67
68            }
69
70
71          }
72  ]
73
74        }
75
76
77      }
78
79
80  }
81
82
83  <!--NeedCopy-->
```

### Administración de aplicaciones cliente para el plug-in de WebEx [Technical Preview]

A partir de la versión 2303, la descarga, la instalación y la actualización automática del plug-in de WebEx se admiten y se gestionan de la misma manera que los plug-ins de Zoom. Para usar esta funcionalidad, se deben incorporar los siguientes ajustes de Global App Configuration para el almacén o cuenta:

```
1  {
2
3    "pluginId": "C03BAE37-F3AC-4D63-8BC1-3C9CD2BC9E8D",
4    "pluginName": "WebEx VDI AutoUpgrade Plugin",
5    "pluginSettings":
6    {
7
8      "delayGroup": "Fast",
9      "deploymentMode": "InstallAndUpdate",
10     "detectRule": "UpgradeCode:{
11   AA2AACDC-D30B-433F-A602-3E25975010A6 }
12   ",
13     "isBlocking": false,
14     "isFTU": false,
```

```
    "maximumAllowedVersion": "3.1.0.24263",
    "minimumAllowedVersion": "0.0.0",
    "stream": "Current",
    "upgradeToLatest": true
   }

 }


<!--NeedCopy-->
```

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Tech Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Puede enviar comentarios sobre esta función a través del formulario de Podio.

## Autenticarse

March 31, 2023

Puede configurar diversos tipos de autenticación para la aplicación Citrix Workspace: autenticación con tarjeta inteligente, autenticación PassThrough de dominio (Single Sign-On o SSON) y autenticación PassThrough con Kerberos.

### Autenticación PassThrough de dominio (Single Sign-On)

La autenticación PassThrough de dominio (Single Sign-On o SSON) permite autenticarse en un dominio y usar Citrix Virtual Apps and Desktops y Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) sin necesidad de autenticarse de nuevo.

> **Nota:**
>
> Si inhabilita la directiva **Habilitar notificaciones de MPR para el sistema** en la plantilla de objetos de directiva de grupo, Windows 11 no admite la función de autenticación de PassThrough de dominio (Single Sign-On).

Cuando está habilitada, la autenticación PassThrough de dominio (Single Sign-On) almacena en caché las credenciales para que pueda conectarse a otras aplicaciones de Citrix sin tener que iniciar sesión cada vez. Para mitigar el riesgo de robo de credenciales, asegúrese de que solo se ejecute en su dispositivo software que cumpla con las directivas corporativas.

Cuando inicia sesión en la aplicación Citrix Workspace, las credenciales se transfieren a StoreFront, junto con las aplicaciones, los escritorios y los parámetros del menú Inicio. Después de configurar el tipo de inicio de sesión Single Sign-On, puede iniciar sesión en la aplicación Citrix Workspace e iniciar sesiones de aplicaciones y escritorios virtuales sin tener que volver a escribir las credenciales.

Todos los exploradores web necesitarán que configure Single Sign-On mediante la plantilla administrativa de objetos de directiva de grupo (GPO). Para obtener más información sobre cómo configurar Single Sign-On mediante la plantilla administrativa de objetos de directiva de grupo (GPO), consulte Configurar Single Sign-On en Citrix Gateway.

Puede configurar el inicio Single Sign-On tanto en una instalación nueva como en una actualización mediante cualquiera de las siguientes opciones:

- Interfaz de la línea de comandos
- Interfaz gráfica (GUI)

> **Nota:**
>
> Es posible que los términos PassThrough de dominio, Single Sign-On y SSON se usen indistintamente en este documento.

#### Configurar Single Sign-On durante una instalación nueva

Para configurar Single Sign-On durante una instalación nueva, siga estos pasos:

1. Configuración en StoreFront.
2. Configure servicios XML de confianza en el Delivery Controller.
3. Modifique parámetros de Internet Explorer.
4. Instale la aplicación Citrix Workspace con Single Sign-On.

#### Configurar Single Sign-On en StoreFront

Single Sign-On le permite autenticarse en un dominio y usar Citrix Virtual Apps and Desktops y Citrix DaaS desde el mismo dominio sin tener que autenticarse de nuevo para cada aplicación o escritorio.

Cuando agrega un almacén mediante la utilidad **Storebrowse**, las credenciales se transfieren al servidor de Citrix Gateway, junto con las aplicaciones y los escritorios enumerados para usted, incluidos los parámetros del menú Inicio. Después de configurar el inicio Single Sign-On, puede agregar el almacén, enumerar sus aplicaciones y escritorios e iniciar los recursos necesarios sin tener que escribir sus credenciales varias veces.

Según la implementación de Citrix Virtual Apps and Desktops, la autenticación Single Sign-On se puede configurar en StoreFront desde la consola de administración.

Utilice esta tabla para ver los diferentes casos de uso y su configuración respectiva:

| Caso de uso | Detalles de configuración | Información adicional |
|---|---|---|
| SSON configurado en StoreFront | Inicie Citrix Studio, vaya a **Almacenes** > **Administrar métodos de autenticación - Almacén** y habilite **PassThrough de dominio**. | Cuando la aplicación Citrix Workspace no está configurada con Single Sign-On, cambia automáticamente el método de autenticación de **PassThrough de dominio** a **Nombre de usuario y contraseña**, si está disponible. |
| Cuando se necesita Workspace para Web | Inicie **Almacenes** > **Sitios de Workspace para Web** > **Administrar métodos de autenticación - Almacén** y habilite **PassThrough de dominio**. | Cuando la aplicación Citrix Workspace no está configurada con Single Sign-On, cambia automáticamente el método de autenticación de **PassThrough de dominio** a **Nombre de usuario y contraseña**, si está disponible. |

#### Configurar Single Sign-On en Citrix Gateway

El inicio Single Sign-On en Citrix Gateway se habilita a través de la plantilla administrativa del GPO.

1. Abra la plantilla administrativa del GPO de la aplicación Citrix Workspace; para ello, ejecute `gpedit.msc`.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Autenticación de usuarios**, y seleccione **Single Sign-On para Citrix Gateway**.
3. Seleccione **Enabled**.
4. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**
5. Reinicie la aplicación Citrix Workspace para que los cambios surtan efecto.

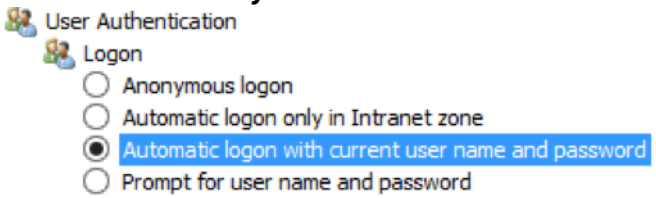
#### Configurar servicios XML de confianza en el Delivery Controller

En Citrix Virtual Apps and Desktops y Citrix DaaS, ejecute el siguiente comando de PowerShell como administrador en el Delivery Controller:

```
asnp Citrix* ; Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True
```

#### Modificar los parámetros de Internet Explorer

1. Agregar el servidor de StoreFront a la lista de sitios de confianza mediante Internet Explorer. Para agregarlo:
   a) Inicie **Opciones de Internet** desde el Panel de control.
   b) Haga clic en **Seguridad** > **Internet local** y, a continuación, haga clic en **Sitios**. Aparecerá la ventana **Intranet local**.
   c) Seleccione **Opciones avanzadas**.
   d) Agregue la URL del FQDN de StoreFront con los protocolos HTTP o HTTPS correspondientes.
   e) Haga clic en **Aplicar** y, a continuación, en **Aceptar.**
2. Modifique los parámetros de **Autenticación del usuario** en **Internet Explorer**. Para modificarlos:
   a) Inicie **Opciones de Internet** desde el Panel de control.
   b) Haga clic en la ficha **Seguridad** > **Intranet local**.
   c) Haga clic en **Nivel personalizado**. Aparece la ventana **Configuración de seguridad: Zona de intranet local**.
   d) En el panel **Autenticación del usuario**, seleccione **Inicio de sesión automático con el nombre de usuario y contraseña actuales**.




   e) Haga clic en **Aplicar** y, a continuación, en **Aceptar.**

#### Configurar Single Sign-On mediante la interfaz de línea de comandos

Instale la aplicación Citrix Workspace con el modificador de línea de comandos `/includeSSON` y reinícielo para que los cambios surtan efecto.

> **Nota:**
>
> Al instalar la aplicación Citrix Workspace para Windows sin el componente Single Sign-On, no se

> permite actualizarla a la versión más reciente de Citrix Workspace con el modificador de línea de comandos `/includeSSON`.

#### Configurar Single Sign-On mediante la GUI

1. Busque el archivo de instalación de la aplicación Citrix Workspace (`CitrixWorkspaceApp.exe`).
2. Haga doble clic en `CitrixWorkspaceApp.exe` para iniciar el instalador.
3. En el asistente de instalación **Habilitar Single Sign-On**, seleccione la opción **Habilitar Single Sign-On**.
4. Haga clic en **Siguiente** y siga las instrucciones para completar la instalación.

Ahora puede iniciar sesión en un almacén existente (o configurar un almacén nuevo) mediante la aplicación Citrix Workspace sin introducir credenciales de usuario.

#### Configurar Single Sign-On en Citrix Workspace para Web

Puede configurar Single Sign-On en Workspace para Web mediante la plantilla administrativa del objeto de directiva de grupo.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace para Web. Para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Autenticación de usuarios**.
3. Seleccione la directiva **Nombre de usuario y contraseña locales** y **habilítela**.
4. Haga clic en **Habilitar autenticación PassThrough**. Esta opción permite a Workspace para Web usar las credenciales de inicio de sesión para autenticarse en el servidor remoto.
5. Haga clic en **Permitir autenticación PassThrough para todas las conexiones ICA**. Esta opción omite las restricciones de autenticación y permite que las credenciales se transfieran en todas las conexiones.
6. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**
7. Reinicie Citrix Workspace para Web para que los cambios surtan efecto.

Verifique si Single Sign-On está habilitado. Para ello, inicie el **Administrador de tareas** y compruebe que el proceso `ssonsvr.exe` se está ejecutando.

#### Configurar Single Sign-On mediante Active Directory

Complete los pasos siguientes para configurar la aplicación Citrix Workspace para la autenticación PassThrough mediante la directiva de grupo de Active Directory. En este caso, puede obtener la autenticación Single Sign-On sin utilizar las herramientas de implementación del software de empresa, como Microsoft System Center Configuration Manager.

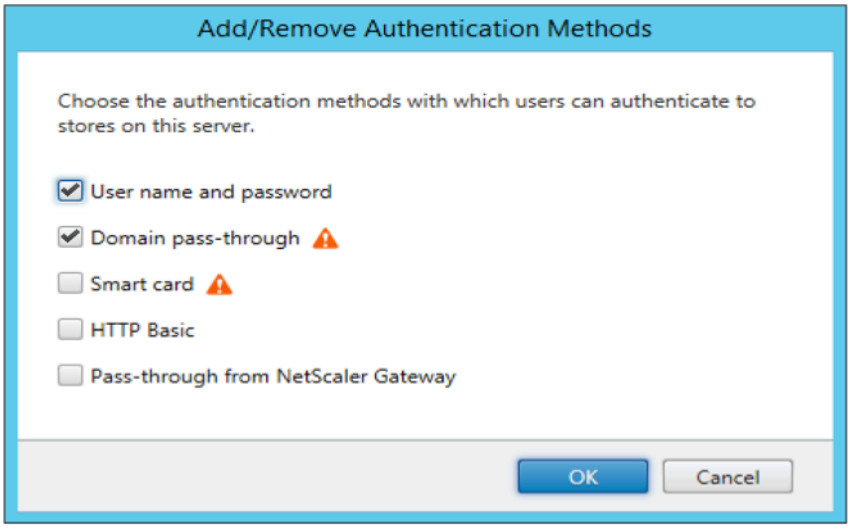
1. Descargue el archivo de instalación de la aplicación Citrix Workspace (CitrixWorkspaceApp.exe) y colóquelo en un recurso compartido de red adecuado. Se debe poder acceder a ese recurso desde las máquinas de destino en las que instale la aplicación Citrix Workspace.
2. Puede obtener la `CheckAndDeployWorkspacePerMachineStartupScript.bat`plantilla desde la página de descargas de la aplicación Citrix Workspace para Windows.
3. Modifique el contenido para adaptarlo a la ubicación y la versión de `CitrixWorkspaceApp.exe`.
4. En la **Consola de administración de directivas de grupo de Active Directory**, escriba `CheckAndDeployWorkspacePerMachineStartupScript.bat` como script de inicio. Para obtener más información sobre cómo implementar los script de inicio, consulte la sección Active Directory.
5. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Agregar o quitar plantillas** para agregar el archivo `receiver.adml`.
6. Después de agregar la plantilla `receiver.adml`, vaya a **Configuración del equipo** > **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Autenticación de usuarios**. Para obtener más información sobre cómo agregar los archivos de plantilla, consulte Plantilla administrativa de objeto de directiva de grupo.
7. Seleccione la directiva **Nombre de usuario y contraseña locales** y **habilítela**.
8. Seleccione **Habilitar autenticación PassThrough** y haga clic en **Aplicar**.
9. Reinicie la máquina para que los cambios surtan efecto.

#### Configurar Single Sign-On en StoreFront

#### Configurar StoreFront

1. Inicie **Citrix Studio** en el servidor de StoreFront y seleccione **Almacenes** > **Administrar métodos de autenticación - Almacén**.
2. Seleccione **PassThrough de dominio**.




### Tokens de autenticación

Los tokens de autenticación se cifran y se almacenan en el disco local para que no tenga que volver a escribir sus credenciales al reiniciar el sistema o la sesión. La aplicación Citrix Workspace ofrece una opción para inhabilitar el almacenamiento de tokens de autenticación en el disco local.

Para mejorar la seguridad, ahora proporcionamos una directiva de objeto de directiva de grupo (GPO) para configurar el almacenamiento de tokens de autenticación.

> **Nota:**
>
> Esta configuración solo se puede aplicar en implementaciones en la nube.

**Para inhabilitar el almacenamiento de tokens de autenticación mediante la directiva de objeto de directiva de grupo (GPO):**

1. Ejecute `gpedit.msc` para abrir la plantilla administrativa de GPO de la aplicación Citrix Workspace.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Autoservicio**.
3. En la directiva **Almacenar tokens de autenticación**, seleccione una de estas opciones:
   - Habilitado: Indica que los tokens de autenticación se almacenan en el disco. De forma predeterminada, habilítela.
   - Inhabilitado: Indica que los tokens de autenticación no se almacenan en el disco. Introduzca de nuevo sus credenciales al reiniciar el sistema o la sesión.
4. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**

A partir de la versión 2106, la aplicación Citrix Workspace ofrece otra opción para inhabilitar el almacenamiento de tokens de autenticación en el disco local. Junto con la configuración de GPO existente,

también puede inhabilitar el almacenamiento de tokens de autenticación en el disco local mediante Global App Configuration Service.

En Global App Configuration Service, establezca el atributo `Store Authentication Tokens` en `False`.

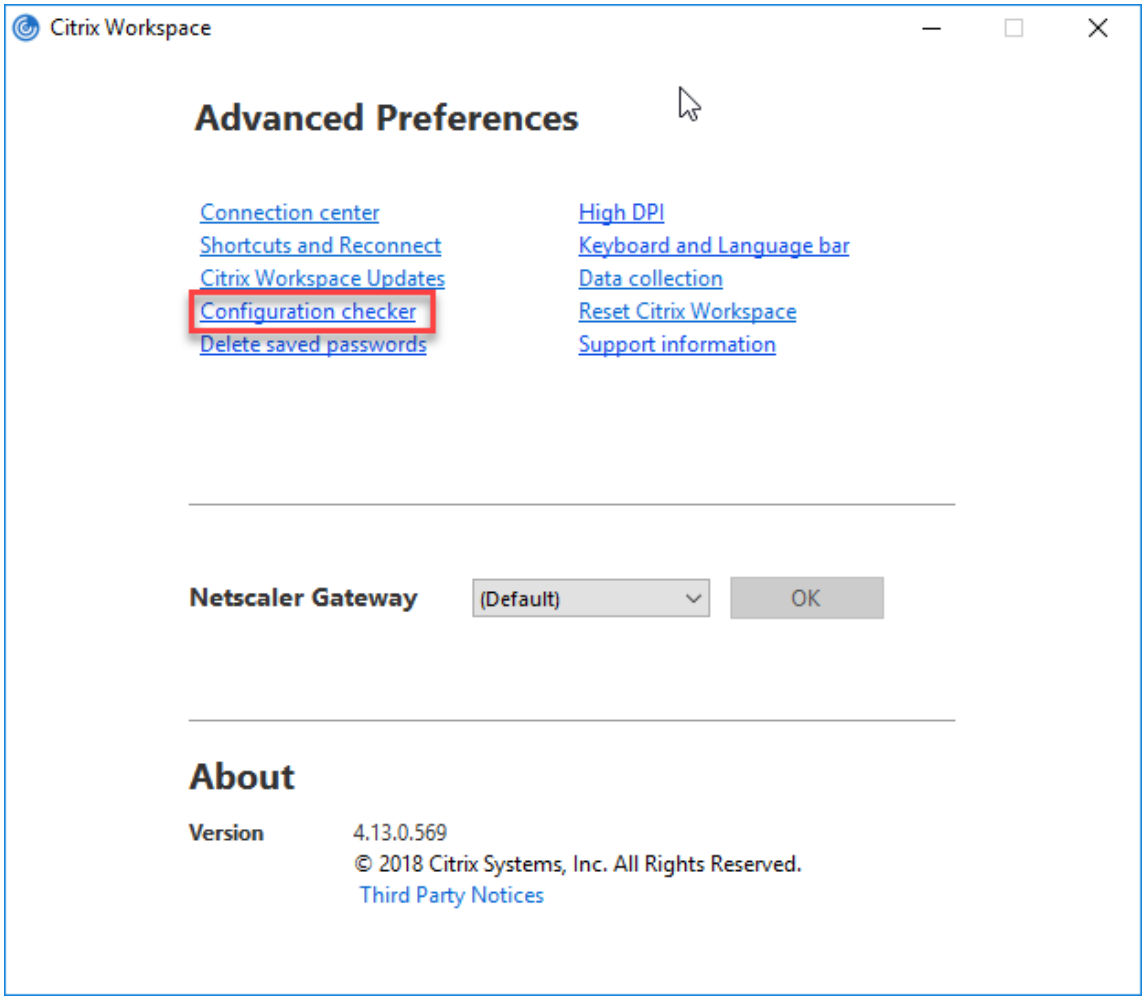
Para obtener más información, consulte la documentación de Global App Configuration Service.

### Configuration Checker

Configuration Checker le permite ejecutar pruebas para comprobar si Single Sign-On está configurado correctamente. Las pruebas se ejecutan en varios puntos de control de la configuración de Single Sign-On y muestran los resultados de la configuración.

1. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace situado en el área de notificaciones y, a continuación, haga clic en **Preferencias avanzadas**.
   Aparecerá el cuadro de diálogo **Preferencias avanzadas**.
2. Haga clic en **Configuration Checker**.
   Aparecerá la ventana **Citrix Configuration Checker**.




3. Seleccione **SSONChecker** desde el panel **Seleccionar**.
4. Haga clic en **Ejecutar**. Aparecerá la barra de progreso, que muestra el estado de la prueba.

La ventana de **Configuration Checker** consta de las siguientes columnas:

1. **Estado:** Muestra el resultado de una prueba en un punto de control concreto.
   - Una marca de verificación (✓) verde indica que el punto de control está configurado correctamente.
   - Una I azul indica información sobre el punto de control.
   - Una X roja indica que ese punto de control no está configurado correctamente.
2. **Proveedor:** Muestra el nombre del módulo en que se ejecuta la prueba. En este caso, Single Sign-On.
3. **Suite:** Indica la categoría de la prueba. Por ejemplo, Instalación.
4. **Prueba:** Indica el nombre de la prueba específica que se ejecuta.
5. **Detalles:** Proporciona información adicional sobre la prueba, independientemente del resul-

tado de esta.

El usuario puede ver más información sobre cada punto de control y los resultados correspondientes.

Se realizan estas pruebas:

1. Instalado con Single Sign-On.
2. Captura de credenciales de inicio de sesión.
3. Registro de proveedores de red: El resultado de la prueba de registro de proveedores de red muestra una marca de verificación verde solo cuando "Citrix Single Sign-On" figura en primer lugar en la lista de proveedores de red. Si Citrix Single Sign-On aparece en algún otro lugar de la lista, el resultado de la prueba Registro de proveedores de red es una barra azul y se ofrece información adicional.
4. Proceso de Single Sign-On en ejecución.
5. Directiva de grupo: De manera predeterminada, esta directiva está configurada en el cliente.
6. Parámetros de Internet para zonas de seguridad: Compruebe que ha agregado la URL del almacén o del servicio XenApp a la lista de zonas de seguridad en las Opciones de Internet.
   Si las zonas de seguridad están configuradas mediante una directiva de grupo, cualquier cambio en la directiva requiere que la ventana **Preferencias avanzadas** se vuelva a abrir para que los cambios surtan efecto y para mostrar el estado correcto de la prueba.
7. Método de autenticación para StoreFront.

> **Nota:**
>
> - Si accede a Workspace para Web, los resultados de la prueba no se aplican.
> - Si la aplicación Citrix Workspace está configurada con varios almacenes, la prueba del método de autenticación se ejecuta en todos los almacenes configurados.
> - Puede guardar como informes los resultados de la prueba. El formato predeterminado del informe es TXT.

#### Ocultar la opción Configuration Checker de la ventana Preferencias avanzadas

1. Abra la plantilla administrativa del GPO de la aplicación Citrix Workspace; para ello, ejecute `gpedit.msc`.
2. Vaya a **Componentes de Citrix** > **Citrix Workspace** > **Autoservicio** > **DisableConfigChecker**.
3. Haga clic en **Habilitado** para ocultar la opción **Configuration Checker** de la ventana **Preferencias avanzadas**.
4. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**
5. Ejecute el comando `gpupdate /force`.

**Limitación:**

Configuration Checker no incluye el punto de control de la configuración de confianza en solicitudes enviadas a XML Service en los servidores de Citrix Virtual Apps and Desktops.

#### Prueba de baliza

La aplicación Citrix Workspace permite realizar una prueba de baliza mediante la herramienta de comprobación de balizas que está disponible como parte de la herramienta **Configuration Checker**. La prueba de baliza ayuda a confirmar si se puede acceder a la baliza (ping.citrix.com). Con esta prueba de diagnóstico, se puede descartar una de las muchas causas posibles para la enumeración lenta de recursos (es decir, que la baliza no esté disponible). Para ejecutar la prueba, haga clic con el botón secundario en la aplicación Citrix Workspace en el área de notificaciones y seleccione **Preferencias avanzadas** > **Configuration Checker**. Seleccione la opción **Beacon Checker** de la lista "Pruebas" y haga clic en **Ejecutar**.

Los resultados de la prueba pueden ser uno de los siguientes:

- Accesible: La aplicación Citrix Workspace puede contactar con la baliza.
- No accesible: La aplicación Citrix Workspace no puede contactar con la baliza.
- Parcialmente accesible: La aplicación Citrix Workspace puede contactar intermitentemente con la baliza.

> **Nota:**
>
> - Los resultados de la prueba no se aplican a Workspace para Web.
> - Puede guardar como informes los resultados de la prueba. El formato predeterminado del informe es TXT.

### Autenticación PassThrough de dominio (Single Sign-On) con Kerberos

Lo descrito en este artículo se aplica solo a conexiones entre la aplicación Citrix Workspace para Windows y StoreFront, Citrix Virtual Apps and Desktops y Citrix DaaS.

La aplicación Citrix Workspace admite Kerberos para la autenticación PassThrough de dominio (Single Sign-On o SSON) en implementaciones que usan tarjetas inteligentes. Kerberos es uno de los métodos de autenticación incluidos en la **autenticación de Windows integrada (IWA)**.

Al habilitarse, Kerberos se autentica sin contraseña en la aplicación Citrix Workspace. Así, impide ataques de tipo troyano que intentan acceder a las contraseñas del dispositivo de usuario. Los usuarios pueden iniciar sesión con cualquier método de autenticación y acceder a recursos publicados; por ejemplo, un autenticador biométrico (un lector de huellas digitales).

Cuando inicie sesión con una tarjeta inteligente en la aplicación Citrix Workspace, StoreFront, Citrix Virtual Apps and Desktops y Citrix DaaS configurados para la autenticación con tarjeta inteligente, la aplicación Citrix Workspace:

1. Captura el PIN de la tarjeta inteligente durante Single Sign-On.
2. Usa IWA (Kerberos) para autenticar al usuario en StoreFront. A continuación, StoreFront proporciona a la aplicación Workspace información sobre las instancias disponibles de Citrix Virtual Apps and Desktops y Citrix DaaS.

> **Nota:**
>
> Habilite Kerberos para evitar una solicitud extra de PIN. Si no se usa la autenticación Kerberos, la aplicación Citrix Workspace se autentica en StoreFront con las credenciales de la tarjeta inteligente.

3. HDX Engine (antes conocido como cliente ICA) pasa el PIN de la tarjeta inteligente al VDA para iniciar la sesión del usuario en la aplicación Citrix Workspace. A continuación, Citrix Virtual Apps and Desktops y Citrix DaaS entregan los recursos solicitados.

Para usar la autenticación Kerberos en la aplicación Citrix Workspace, compruebe si la configuración de Kerberos cumple estos requisitos.

- Kerberos solo funciona entre la aplicación Citrix Workspace y los servidores que pertenecen a los mismos dominios de Windows o a dominios que son de confianza. Se confía en los servidores para la delegación, una opción que se configura a través de la herramienta de administración de usuarios y equipos de Active Directory.
- Kerberos debe estar habilitado tanto en el dominio como en Citrix Virtual Apps and Desktops y en Citrix DaaS. Para mayor seguridad y para asegurarse de que se utiliza Kerberos, inhabilite las demás opciones que no sean Kerberos IWA en el dominio.
- El inicio de sesión con Kerberos no está disponible para conexiones de Servicios de escritorio remoto configuradas para usar la autenticación básica, para usar siempre la información de inicio de sesión especificada o para pedir siempre una contraseña.

> **Advertencia:**
>
> Es posible que el uso incorrecto del Editor del Registro del sistema cause problemas graves que puedan obligarle a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de un uso incorrecto del Editor del Registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

#### Autenticación PassThrough de dominio (Single Sign-On) con Kerberos para usarla con tarjetas inteligentes

Antes de continuar, consulte la sección Proteger la implementación en el documento de Citrix Virtual Apps and Desktops.

Cuando instale la aplicación Citrix Workspace para Windows, incluya la opción siguiente en la línea de comandos:

- `/includeSSON`

  Esta opción instala el componente Single Sign-On en el equipo unido a un dominio, lo que habilita a Citrix Workspace para autenticarse en StoreFront mediante IWA (Kerberos). El compo-

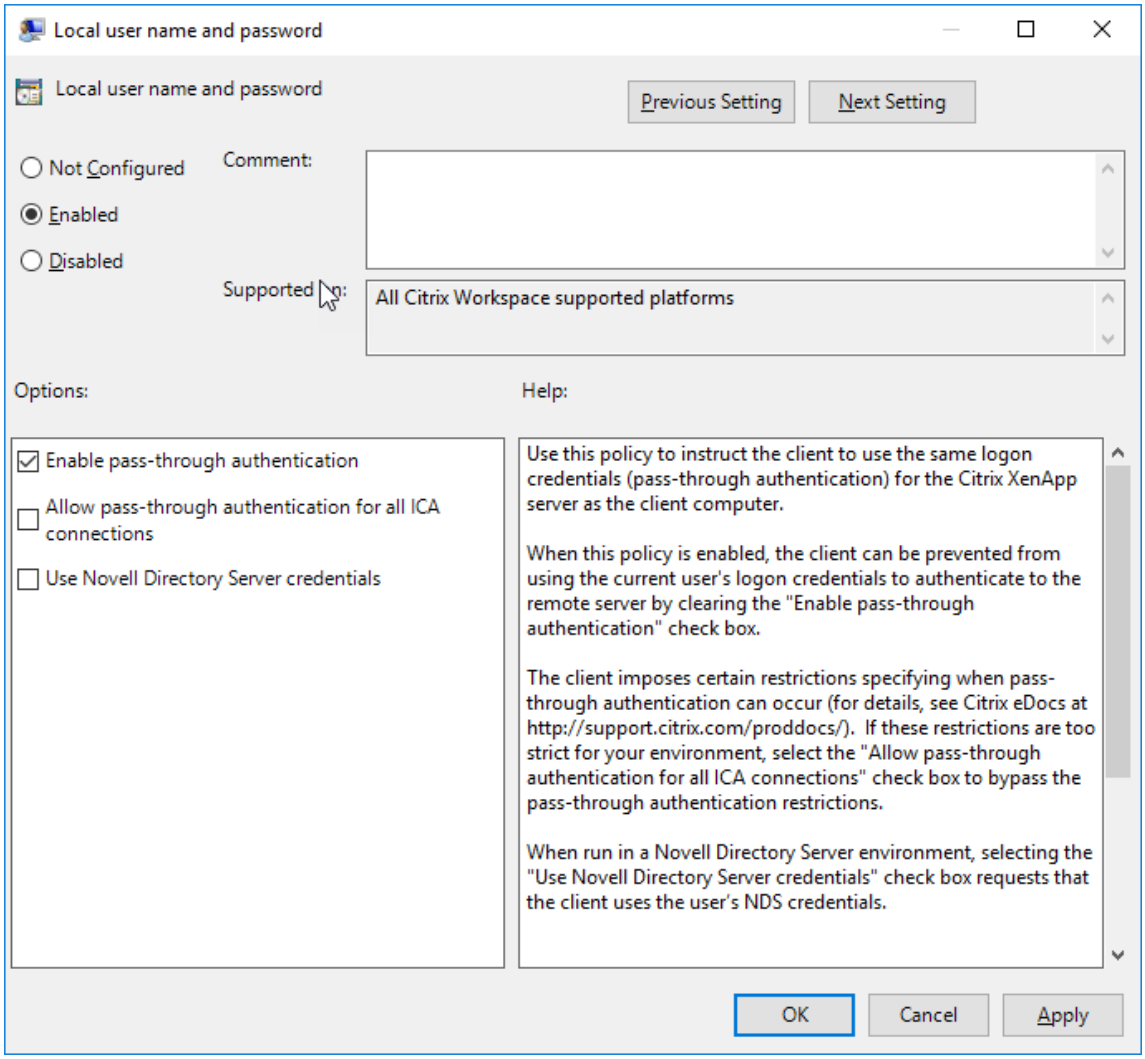
nente Single Sign-On guarda el PIN de la tarjeta inteligente que el motor HDX utiliza cuando comunica de forma remota el hardware de la tarjeta inteligente y las credenciales a Citrix Virtual Apps and Desktops y Citrix DaaS. Citrix Virtual Apps and Desktops y Citrix DaaS seleccionan automáticamente un certificado desde la tarjeta inteligente y obtienen el PIN desde el motor HDX.

La opción relacionada `ENABLE_SSON` está habilitada de forma predeterminada.

Si una directiva de seguridad le impide habilitar el inicio Single Sign-On en un dispositivo, configure la aplicación Citrix Workspace mediante la plantilla administrativa del objeto de directiva de grupo.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. Elija **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Autenticación de usuarios** > **Nombre de usuario y contraseña locales**.
3. Seleccione **Habilitar autenticación PassThrough**.
4. Reinicie la aplicación Citrix Workspace para que los cambios surtan efecto.




**Para configurar StoreFront:**

Durante la configuración del servicio de autenticación en el servidor de StoreFront, seleccione la opción **PassThrough de dominio**. Este parámetro habilita la autenticación de Windows integrada (IWA). No es necesario seleccionar la opción “Tarjeta inteligente” a menos que también tenga clientes que no estén unidos a un dominio conectándose a StoreFront con tarjeta inteligente.

Para obtener más información sobre el uso de tarjetas inteligentes con StoreFront, consulte Configurar el servicio de autenticación en la documentación de StoreFront.

### Compatibilidad del Acceso condicional con Azure Active Directory

El Acceso condicional es una herramienta utilizada por Azure Active Directory para aplicar directivas de organización. Los administradores de Workspace pueden configurar y aplicar directivas de acceso condicional de Azure Active Directory a usuarios que se autentican en la aplicación Citrix Workspace. La máquina Windows que ejecute la aplicación Workspace debe tener instalada la versión 99 de Mi-

crosoft Edge WebView2 Runtime o una versión posterior.

Para obtener información e instrucciones completas sobre cómo configurar directivas de acceso condicional con Azure Active Directory, consulte la **documentación sobre el Acceso condicional de Azure AD** en *docs.microsoft.com/es-es/azure/active-directory/conditional-access/*.

> **Nota:**
>
> Esta función solo está disponible en implementaciones de Workspace (Cloud).

### Compatibilidad con métodos de autenticación modernos para almacenes de StoreFront

La aplicación Citrix Workspace 2303 para Windows admite métodos de autenticación modernos para los almacenes de StoreFront. Puede autenticarse en los almacenes de Citrix StoreFront de cualquiera de las siguientes formas:

- Con claves de seguridad de Windows Hello y FIDO2. Para obtener más información, consulte Otras formas de autenticarse.
- Single Sign-On (SSO) en los almacenes de Citrix StoreFront desde máquinas unidas a Azure Active Directory (AAD) con AAD como proveedor de identidades. Para obtener más información, consulte Otras formas de autenticarse.
- Los administradores de Workspace pueden configurar y aplicar directivas de acceso condicional de Azure Active Directory para usuarios que se autentican en los almacenes de Citrix StoreFront. Para obtener más información, consulte Compatibilidad con el acceso condicional con Azure AD.

Para habilitar esta funcionalidad, debe utilizar Microsoft Edge WebView2 como explorador subyacente para la autenticación directa de StoreFront y la puerta de enlace.

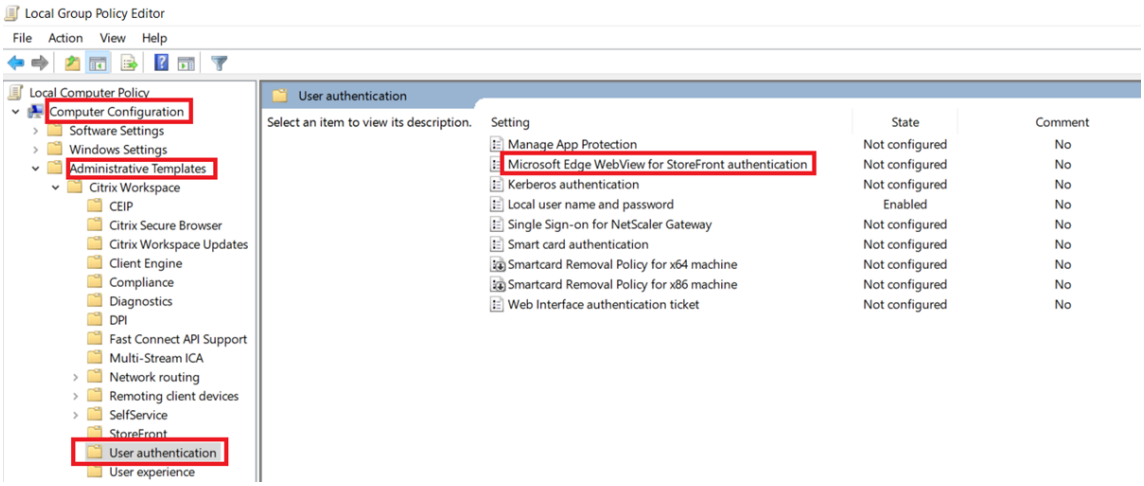
> **Nota:**
>
> La versión de Microsoft Edge WebView2 Runtime debe ser 102 o posterior.

Puede habilitar métodos de autenticación modernos para los almacenes de StoreFront con la plantilla de objeto de directiva de grupo.

Para habilitar esta funcionalidad:

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Citrix Workspace** > **Autenticación de usuarios**.
3. Haga clic en la directiva de **autenticación de Microsoft Edge WebView para StoreFront** y configúrela en **Habilitada**.




4. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Cuando esta directiva está inhabilitada, la aplicación Citrix Workspace utiliza Internet Explorer WebView. Como resultado, no se admiten los métodos de autenticación modernos para los almacenes de Citrix StoreFront.

### Otras formas de autenticarse

Puede configurar estos mecanismos de autenticación con la aplicación Citrix Workspace. Para que estos mecanismos de autenticación funcionen como es debido, la máquina Windows que ejecuta la aplicación Workspace debe tener instalada la versión 99 de Microsoft Edge WebView2 Runtime o una versión posterior.

1. Autenticación por Windows Hello: Para obtener instrucciones sobre cómo configurar la autenticación por Windows Hello, consulte **Configure Windows Hello for Business Policy settings - Certificate Trust** en _docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-cert-trust-policy-settings.

   > **Nota:**
   >
   > No se admite la autenticación basada en Windows Hello con PassThrough de dominio (Single Sign-On o SSON).

2. Autenticación por claves de seguridad FIDO2: Las claves de seguridad FIDO2 ofrecen un método intuitivo para que los empleados se autentiquen sin introducir nombres de usuario ni contraseñas. Puede configurar la autenticación por claves de seguridad FIDO2 en Citrix Workspace. Si quiere que los usuarios se autentiquen en Citrix Workspace con su cuenta de Azure AD mediante una clave de seguridad FIDO2, consulte **Habilitación del inicio de sesión con clave de seguridad sin contraseña** en *docs.microsoft.com/es-es/azure/active-directory/authentication/howto-authentication-passwordless-security-key*.

3. También puede configurar Single Sign-On (SSO) en la aplicación Citrix Workspace desde máquinas unidas a Microsoft Azure Active Directory (AAD) con AAD como un proveedor de identidades Para obtener más información detallada sobre la configuración de Azure Active Directory Domain Services, consulte **Configurar Azure Active Directory Domain Services** en *docs.microsoft.com/es-es/azure/active-directory-domain-services/overview*. Para obtener información sobre cómo conectar Azure Active Directory a Citrix Cloud, consulte Conectar Azure Active Directory a Citrix Cloud.

### Tarjeta inteligente

La aplicación Citrix Workspace para Windows admite la siguiente autenticación con tarjeta inteligente:

- **Autenticación PassThrough (Single Sign-On):** La autenticación PassThrough captura las credenciales de la tarjeta inteligente cuando los usuarios inician sesión en la aplicación Citrix Workspace. La aplicación Citrix Workspace usa las credenciales capturadas de la siguiente manera:
  - Los usuarios de dispositivos unidos a un dominio que inician sesión en la aplicación Citrix Workspace con una tarjeta inteligente pueden iniciar aplicaciones y escritorios virtuales sin necesidad de volver a autenticarse.
  - Los usuarios de dispositivos no unidos a ningún dominio que inician sesión en la aplicación Citrix Workspace con credenciales de tarjeta inteligente deben escribir de nuevo sus credenciales para poder iniciar una aplicación o escritorio virtual.

  La autenticación PassThrough debe configurarse tanto en StoreFront como en la aplicación Citrix Workspace.
- **Autenticación bimodal:** La autenticación bimodal ofrece a los usuarios la opción de usar una tarjeta inteligente o escribir su nombre de usuario y contraseña. Esta función es efectiva cuando no se puede usar la tarjeta inteligente; por ejemplo, cuando el certificado de inicio de sesión ha caducado. Para permitir la autenticación bimodal, deben configurarse almacenes dedicados para cada sitio siguiendo el método de **DisableCtrlAltDel** establecido en el valor **False** para permitir el uso de tarjetas inteligentes. La autenticación bimodal requiere una configuración de StoreFront.

  Con la autenticación bimodal, el administrador de StoreFront puede permitir autenticarse tanto con nombre y contraseña como con tarjeta inteligente en un mismo almacén. Para ello, el administrador debe seleccionar estas dos opciones en la consola de StoreFront. Consulte la documentación de StoreFront.
- **Varios certificados:** Pueden emplearse varios certificados para una única tarjeta inteligente, y también si se utilizan varias tarjetas inteligentes. Cuando se inserta una tarjeta inteligente en el

lector de tarjetas, los certificados se aplican a todas las aplicaciones ejecutadas en el dispositivo del usuario, incluida la aplicación Citrix Workspace.

- **Autenticación por certificado del cliente:** La autenticación por certificado del cliente requiere la configuración de Citrix Gateway y StoreFront.
  - Para acceder a StoreFront a través de Citrix Gateway, debe volver a autenticarse después de extraer la tarjeta inteligente.
  - Cuando la configuración SSL de Citrix Gateway está definida como **Autenticación por certificado de cliente obligatoria**, la operación es más segura. No obstante, la autenticación por certificado de cliente obligatoria no es compatible con la autenticación bimodal.
- **Sesiones de doble salto:** Si es necesario el doble salto, se establece una conexión entre la aplicación Citrix Workspace y el escritorio virtual del usuario.
- **Aplicaciones habilitadas para tarjeta inteligente:** Las aplicaciones habilitadas para tarjeta inteligente, como Microsoft Outlook y Microsoft Office, permiten a los usuarios cifrar o firmar digitalmente los documentos disponibles en las sesiones de aplicaciones y escritorios virtuales.

**Limitaciones:**

- Los certificados deben guardarse en una tarjeta inteligente, no en el dispositivo del usuario.
- La aplicación Citrix Workspace no guarda la elección de certificado del usuario, pero guarda el PIN si se configura así. El PIN se almacena en caché solo en la memoria no paginada durante la sesión del usuario. No se guarda en el disco.
- La aplicación Citrix Workspace no se reconecta a sesiones cuando se inserta una tarjeta inteligente.
- Cuando está configurada para la autenticación con tarjeta inteligente, la aplicación Citrix Workspace no admite ni el Preinicio de sesiones ni Single Sign-On en redes privadas virtuales (VPN). Para usar una VPN con la autenticación con tarjeta inteligente, instale Citrix Gateway Plug-in. Inicie sesión en una página web con sus tarjetas inteligentes y sus PIN para autenticarse en cada paso. La autenticación PassThrough en StoreFront con Citrix Gateway Plug-in no está disponible para los usuarios de tarjeta inteligente.
- Las comunicaciones de Citrix Workspace Updater con citrix.com y Merchandising Server no son compatibles con la autenticación por tarjeta inteligente en Citrix Gateway.

> **Advertencia**
>
> Algunas configuraciones requieren modificaciones del Registro. Es posible que el uso incorrecto del Editor del Registro del sistema cause problemas que puedan requerir la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de un uso incorrecto del Editor del Registro puedan resolverse. Haga una copia de seguridad del Registro antes de modificarlo.

**Para habilitar la autenticación Single Sign-On para tarjeta inteligente:**

Para configurar la aplicación Citrix Workspace para Windows, incluya la siguiente opción de línea de comandos cuando la instale:

- `ENABLE_SSON=Yes`

  Single Sign-On es otro término para el paso de credenciales/autenticación PassThrough. Habilitar este parámetro impide que la aplicación Citrix Workspace muestre una segunda solicitud de PIN.

- En el Editor del Registro, vaya a esta ruta de acceso y establezca la cadena `SSONCheckEnabled` en `False` si no instaló el componente Single Sign-On.

  `HKEY_CURRENT_USER\Software{ Wow6432 } \Citrix\AuthManager\protocols\integratedwindows\`

  `HKEY_LOCAL_MACHINE\Software{ Wow6432 } \Citrix\AuthManager\protocols\integratedwindows\`

  La clave impide que Authentication Manager de la aplicación Citrix Workspace busque el componente Single Sign-On y permite que la aplicación Citrix Workspace se autentique en StoreFront.

Para habilitar la autenticación en StoreFront con tarjeta inteligente en lugar de Kerberos, instale la aplicación Citrix Workspace para Windows con las siguientes opciones de la línea de comandos.

- `/includeSSON` instala Single Sign-On (autenticación PassThrough). Habilita el almacenamiento en caché de credenciales y el uso de la autenticación PassThrough de dominio.
- Si el usuario inicia sesión en el dispositivo de punto final con otro método de autenticación como, por ejemplo, nombre de usuario y contraseña, la línea de comandos es:

  `/includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No`

Este tipo de autenticación evita la captura de las credenciales al iniciar sesión y permite que la aplicación Citrix Workspace almacene el PIN durante el inicio de sesión en la aplicación Citrix Workspace.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. Vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Autenticación de usuarios** > **Nombre de usuario y contraseña locales**.
3. Seleccione **Habilitar autenticación PassThrough**. Dependiendo de la configuración y los parámetros de seguridad, seleccione la opción **Permitir autenticación PassThrough para todas las conexiones ICA** para que la autenticación PassThrough funcione.

**Para configurar StoreFront:**

- Al configurar el servicio de autenticación, marque la casilla **Tarjeta inteligente**.

Para obtener más información sobre el uso de tarjetas inteligentes con StoreFront, consulte Configurar el servicio de autenticación en la documentación de StoreFront.

**Para habilitar los dispositivos de los usuarios para el uso de tarjetas inteligentes:**

1. Importe el certificado raíz de la entidad de certificación en el almacén de claves del dispositivo.
2. Instale el middleware de su proveedor de servicios criptográficos.
3. Instale y configure la aplicación Citrix Workspace.

**Para cambiar cómo se seleccionan los certificados:**

De manera predeterminada, si hay varios certificados válidos, la aplicación Citrix Workspace pide al usuario que elija uno de la lista. En su lugar, puede configurar la aplicación Citrix Workspace para que use el certificado predeterminado (por proveedor de tarjeta inteligente) o el certificado con la fecha de caducidad más lejana. Si no hay certificados de inicio de sesión válidos, se notifica esto al usuario y se le da la opción de usar un método de inicio de sesión alternativo, si hay alguno disponible.

Un certificado válido debe reunir estas características:

- La fecha y hora actuales según el reloj del equipo local está dentro del período de validez del certificado.
- La clave pública **Sujeto** debe usar el algoritmo de RSA y tener una longitud de 1024, 2048 o 4096 bits.
- El uso de claves debe incluir la firma digital.
- Las sesiones de Citrix Virtual Apps se cierran al extraer la tarjeta inteligente.
- El campo "Uso mejorado de claves" debe incluir Inicio de sesión de tarjeta inteligente y Autenticación del cliente o Todos los usos de la clave.
- Una de las entidades de certificación en la cadena de emisores del certificado debe coincidir con uno de los nombres distintivos (DN) permitidos que haya enviado el servidor durante el protocolo de enlace TLS.

Cambie el modo en que se seleccionan los certificados mediante uno de estos métodos:

- En la línea de comandos de la aplicación Citrix Workspace, especifique la opción `AM_CERTIFICATESELECTI` `={ Prompt | SmartCardDefault | LatestExpiry }`.

  La opción predeterminada es "Prompt" (Preguntar). Para `SmartCardDefault` o `LatestExpiry`, si hay varios certificados que cumplen esos criterios, la aplicación Citrix Workspace pide al usuario que elija un certificado.

- Agregue el siguiente valor a la clave de Registro `HKEY_CURRENT_USER OR HKEY_LOCAL_MACHINE \Software\[Wow6432Node\Citrix\AuthManager`: CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry }.

Los valores definidos en `HKEY_CURRENT_USER` tienen preferencia sobre los valores definidos en `HKEY_LOCAL_MACHINE` para facilitar al usuario la selección de un certificado.

**Para usar solicitudes de PIN del proveedor de servicios criptográficos (CSP):**

De manera predeterminada, los diálogos de PIN que se presentan a los usuarios provienen de la aplicación Citrix Workspace para Windows, en lugar de venir del proveedor CSP (Cryptographic Service

Provider) de la tarjeta inteligente. La aplicación Citrix Workspace pide a los usuarios que escriban un PIN cuando es necesario, y luego pasa el PIN al proveedor CSP de la tarjeta inteligente. Si el sitio o la tarjeta inteligente tienen unos requisitos de seguridad más estrictos (por ejemplo, prohibir el almacenamiento del PIN en caché por proceso o por sesión), puede configurar la aplicación Citrix Workspace para que use los componentes del CSP para gestionar las entradas de PIN, incluida la solicitud del PIN.

Cambie el modo en que se gestiona la introducción de PIN mediante uno de estos métodos:

- En la línea de comandos de la aplicación Citrix Workspace, especifique la opción `AM_SMARTCARDPINENTRY=CSP`.
- Agregue el siguiente valor a la clave de Registro `HKEY_LOCAL_MACHINE\Software\[Wow6432Node\Citrix\AuthManager`: SmartCardPINEntry=CSP.

#### Cambios en la extracción y la compatibilidad de tarjetas inteligentes

Las sesiones de Citrix Virtual Apps se cierran al extraer la tarjeta inteligente. Si la aplicación Citrix Workspace está configurada con tarjeta inteligente como método de autenticación, configure la directiva correspondiente en la aplicación Citrix Workspace para Windows para que se aplique el cierre de las sesiones de Citrix Virtual Apps. La sesión del usuario sigue abierta en la aplicación Citrix Workspace.

**Limitación:**

Cuando inicia sesión en el sitio de la aplicación Citrix Workspace mediante la autenticación con tarjeta inteligente, el nombre de usuario aparece como **Conectado**.

#### Tarjeta inteligente rápida

La tarjeta inteligente rápida es una mejora con respecto a la redirección HDX existente de tarjetas inteligentes basada en PC/SC. Mejora el rendimiento cuando se usan tarjetas inteligentes en entornos WAN con latencia alta.

Las tarjetas inteligentes rápidas solo se admiten en Linux VDA.

**Para habilitar el inicio de sesión con tarjeta inteligente rápida en la aplicación Citrix Workspace:**

El inicio de sesión con tarjeta inteligente rápida está habilitado de forma predeterminada en VDA e inhabilitado de forma predeterminada en la aplicación Citrix Workspace. Para habilitarlo, incluya el siguiente parámetro en el archivo **`default.ica`** del sitio asociado de StoreFront:

```
copy[WFClient]
SmartCardCryptographicRedirection=On
<!--NeedCopy-->
```

**Para inhabilitar el inicio de sesión con tarjeta inteligente rápida en la aplicación Citrix Workspace:**

Para inhabilitar el inicio de sesión con tarjeta inteligente rápida en la aplicación Citrix Workspace, quite el parámetro `SmartCardCryptographicRedirection` del archivo **`default`**`.ica` del sitio asociado de StoreFront.

Para obtener más información, consulte Tarjetas inteligentes.

### Autenticación silenciosa para Citrix Workspace

La aplicación Citrix Workspace presenta una directiva de objeto de directiva de grupo (GPO) para habilitar la autenticación silenciosa en Citrix Workspace. Esta directiva permite a la aplicación Citrix Workspace iniciar sesión en Citrix Workspace automáticamente al iniciar el sistema. Utilice esta directiva solo cuando la autenticación PassThrough de dominio (Single Sign-On o SSON) esté configurada para Citrix Workspace en dispositivos unidos a un dominio.

Para que esta directiva funcione, se deben cumplir los siguientes criterios:

- Single Sign-On debe estar habilitado.
- La clave `SelfServiceMode` debe establecerse en `Off` en el editor del Registro.

**Habilitar la autenticación silenciosa:**

1. Ejecute `gpedit.msc` para abrir la plantilla administrativa de GPO de la aplicación Citrix Workspace.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Citrix Workspace** > **Autoservicio**.
3. Haga clic en la directiva **Autenticación silenciosa para Citrix Workspace** y **habilítela**.
4. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**

### Impedir que la aplicación Citrix Workspace para Windows almacene en caché contraseñas y nombres de usuario

De manera predeterminada, la aplicación Citrix Workspace para Windows rellena el formulario automáticamente con el último nombre de usuario que se utilizó. Para que el campo de nombre de usuario no se rellene automáticamente, modifique el Registro en el dispositivo del usuario:

1. Cree un valor REG_SZ HKLM\SOFTWARE\Citrix\AuthManager\RememberUsername.
2. Establezca su valor en “false”.

Para inhabilitar la casilla **Recordar mi contraseña** e impedir el inicio de sesión automático, cree la siguiente clave de Registro en el equipo cliente en el que esté instalada la aplicación Citrix Workspace para Windows:

- Ruta: HKLM\Software\wow6432node\Citrix\AuthManager

- Tipo: REG_SZ
- Nombre: SavePasswordMode
- Valor: Never

> **Nota:**
>
> El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden hacer necesaria la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Para evitar el almacenamiento en caché de las credenciales de los almacenes de StoreFront, consulte Impedir que la aplicación Citrix Workspace para Windows almacene en caché contraseñas y nombres de usuario en la documentación de StoreFront.

## Tabla de acceso de PassThrough de dominio

February 17, 2023

Si utiliza Citrix Workspace y quiere usar PassThrough de dominio, las tablas de las subsecciones describen los diferentes casos y si puede usar o no PassThrough de dominio para cada caso.

Los diferentes elementos de los encabezados de las tablas y la información adicional sobre los elementos de los encabezados son los siguientes:

- Dispositivo de punto final unido a: Indica el directorio al que se une el dispositivo de punto final. El directorio proporciona control de acceso a recursos locales. Puede ser Active Directory (AD) local, Azure Active Directory (AAD) o híbrido.
- Proveedor de identidades (IdP): Entidad utilizada para proporcionar servicios de autenticación a Citrix Workspace. Le permite conectarse a los recursos.
- Servicio de autenticación federada (FAS): Para obtener más información, consulte Habilitar Single Sign-On para espacios de trabajo con Citrix Federated Authentication Service.
- Virtual Delivery Agent (VDA): Para obtener más información, consulte Instalar VDA.
- VDA unido a: Indica el directorio al que está unido el dispositivo VDA. Para obtener más información, consulte Administración de acceso e identidad.
- Single Sign-On (SSO) en Citrix Workspace/VDA: El valor Sí o No indica si se admite PassThrough de dominio a Citrix Workspace o VDA.
- Aplicación Citrix Workspace: Para aplicar Single Sign-On, consulte Configurar Single Sign-On durante una instalación nueva en Autenticación de PassThrough de dominio.

> **Nota:**
>
> Es posible que necesite la versión más reciente de la aplicación Citrix Workspace para poder usar PassThrough de dominio en algunos de estos casos.

### PassThrough de dominio para Citrix Workspace

| Dispositivo de punto final unido a | IdP | VDA unido a | SSO en Citrix Workspace | SSO en VDA | Documentación |
|---|---|---|---|---|---|
| AD | Dispositivo Citrix Gateway local | AD | Sí | Aplicación Citrix Workspace/-FAS | PassThrough de dominio a Citrix Workspace con Citrix Gateway local como proveedor de identidades. |

| Dispositivo de punto final unido a | IdP | VDA unido a | SSO en Citrix Workspace | SSO en VDA | Documentación |
|---|---|---|---|---|---|
| AD | Autenticación adaptable | AD | Sí | Aplicación Citrix Workspace/-FAS | Para configurar la autenticación adaptable, consulte Servicio de autenticación adaptable y siga las instrucciones de PassThrough de dominio a Citrix Workspace mediante Citrix Gateway local como proveedor de identidades. |
| AD | Citrix Gateway federado en otro IdP (AAD/Okta) | AD | Sí | Aplicación Citrix Workspace/-FAS | Configure el IdP mediante Configure SAML Single Sign-On y consulte la docu-mentación del IdP utilizado para configurar PassThrough de dominio. |

| Dispositivo de punto final unido a | IdP | VDA unido a | SSO en Citrix Workspace | SSO en VDA | Documentación |
|---|---|---|---|---|---|
| AD | Okta | AD | Sí | Aplicación Citrix Workspace/-FAS | PassThrough de dominio a Citrix Workspace con Okta como proveedor de identidades. |
| Unido a AD/híbrido | AAD (AD con AAD Connect) | AD | Sí | Aplicación Citrix Workspace/-FAS ** | PassThrough de dominio a Citrix Workspace con Azure Active Directory como proveedor de identidades. |
| AD | Un proveedor de identidades basado en SAML (por ejemplo: ADFS) | AD | Sí | Aplicación Citrix Workspace/-FAS | Consulte Conectar SAML como proveedor de identidades con Citrix Cloud y consulte la documentación del proveedor de identidades utilizado para configurar PassThrough de dominio. |

| Dispositivo de punto final unido a | IdP | VDA unido a | SSO en Citrix Workspace | SSO en VDA | Documentación |
|---|---|---|---|---|---|
| AD | AD | AD | No | No se admite | NA |
| AD | AD+OTP | AD | No | No se admite | NA |
| AD | AAD | AAD | No | No se admite | NA |
| AAD | AAD sin AD local | AD | Sí | FAS | Citrix Workspace usa Microsoft Edge WebView, que permite SSO en Workspace. SSO en VDA se puede usar a través de FAS. Para obtener más información, consulte Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix. |

| Dispositivo de punto final unido a | IdP | VDA unido a | SSO en Citrix Workspace | SSO en VDA | Documentación |
|---|---|---|---|---|---|
| AAD | AAD | AAD | Sí | El usuario debe introducir las credenciales. | Citrix Workspace usa Microsoft Edge WebView, que permite SSO en Workspace. No se admite SSO en VDA. |
| No unido a ningún dominio | IdP que admite la autenticación sin contraseña: Enlace | AD | No | FAS | Citrix Workspace usa Microsoft Edge WebView, que permite SSO en Workspace. SSO en VDA se puede usar a través de FAS. Para obtener más información, consulte Otras maneras de autenticarse en Citrix Workspace. |

**Notas:**

- El cliente debe poder contactarse en AD para que Kerberos funcione.
- **Citrix Single Sign-On (SSONSVR.exe) solo funciona con el nombre de usuario o la con-

traseña en el cliente. Si el usuario usa Windows Hello para iniciar sesión, se necesita FAS.
- Es posible que la autenticación no sea completamente silenciosa en la nube si se habilita LLT o si se configura la directiva de aceptación de usuarios finales.
- Se recomienda configurar FAS, ya que se aplica a plataformas que no son Windows.

### PassThrough de dominio para StoreFront

| Dispositivo de punto final unido a | IdP | VDA unido a | SSO en Citrix Workspace | SSO en VDA | Documentación |
|---|---|---|---|---|---|
| AD | StoreFront | AD | Sí | Aplicación Citrix Workspace | Autenticación PassThrough de dominio |
| Unido a AD/híbrido/Windows Hello para empresas | StoreFront | AD | Sí(1) | Aplicación Citrix Workspace/-FAS(2) | Autenticación de PassThrough de dominio y Habilitar Single Sign-On para espacios de trabajo con Citrix Federated Authentication Service |
| AD | Citrix Gateway: Autenticación avanzada | AD | Sí | Aplicación Citrix Workspace(3)) | |
| AD | Citrix Gateway: Autenticación básica | AD | Sí | Aplicación Citrix Workspace(4) | Autenticación PassThrough de dominio. |

**Notas:**

1. En el Editor del Registro, vaya a esta ruta de acceso y establezca la cadena `SSONCheckEnabled`

en `False` si no instaló el componente Single Sign-On.

`HKEY_LOCAL_MACHINE\Software{ Wow6432 } \Citrix\AuthManager\protocols\integratedwindows\`

The key prevents the Citrix Workspace app authentication manager from checking for the single sign-on component and allows Citrix Workspace app to authenticate to StoreFront.

2. Si usa Windows Hello para iniciar sesión, se necesitan FAS y la configuración del Registro para habilitar SSO.
3. Necesita que el cliente pueda contactarse en AD, ya que utiliza Kerberos.
4. Funciona incluso si el cliente no puede contactarse en AD. No se usa Kerberos.

## PassThrough de dominio a Citrix Workspace con Citrix Gateway local como proveedor de identidades

January 18, 2023

> **Importante:**
>
> Este artículo ayuda a configurar la autenticación PassThrough de dominio. Si ya ha configurado Gateway local como proveedor de identidades, vaya a la sección Configurar PassThrough de dominio como método de autenticación en Citrix Gateway.

Citrix Cloud admite el uso de dispositivos Citrix Gateway locales como proveedores de identidades para autenticar a los suscriptores que inician sesión en sus espacios de trabajo.

Con la autenticación de Citrix Gateway, puede:

- Siga autenticando a los usuarios a través de su dispositivo Citrix Gateway existente para que puedan acceder a los recursos de la implementación local de Virtual Apps and Desktops a través de Citrix Workspace.
- Utilice las funciones de autenticación, autorización y auditoría de Citrix Gateway con Citrix Workspace.
- Proporcione a los usuarios acceso a los recursos que necesitan a través de Citrix Workspace con funciones como la autenticación PassThrough, las tarjetas inteligentes, los tokens seguros, las directivas de acceso condicional, la federación y muchas otras.

La autenticación de Citrix Gateway se puede utilizar con las siguientes versiones de producto:

- Citrix Gateway 13.1.4.43 Advanced Edition o posterior

**Requisitos previos:**

- Cloud Connectors: Necesita al menos dos (2) servidores donde instalar el software Citrix Cloud Connector.
- Active Directory y asegúrese de que el dominio esté registrado.
- Requisitos de Citrix Gateway
  - Use directivas avanzadas en la puerta de enlace local porque las directivas clásicas han dejado de utilizarse.
  - Cuando configure Gateway para autenticar suscriptores en Citrix Workspace, la puerta de enlace actúa como un proveedor de OpenID Connect. Los mensajes entre Citrix Cloud y Gateway se ajustan al protocolo OIDC, que implica la firma digital de tokens. Por lo tanto, debe configurar un certificado para firmar estos tokens.
  - Sincronización del reloj: Citrix Gateway debe sincronizarse con la hora NTP.

Para obtener más información, consulte Requisitos previos en la documentación de Citrix Cloud.

Antes de crear la directiva de IdP de OAuth, debe configurar Citrix Workspace o Cloud para que usen Gateway como opción de autenticación en el IdP (proveedor de identidades). Para obtener más información sobre cómo configurarlo, consulte Conectar un dispositivo Citrix Gateway local como proveedor de identidades con Citrix Cloud. Cuando completa la configuración, se generan el ID de cliente, el secreto y la URL de redireccionamiento necesarios para crear la directiva de IdP de OAuth.

PassThrough de dominio para Workspace para web está habilitado si utiliza Internet Explorer, Microsoft Edge, Mozilla Firefox y Google Chrome. PassThrough de dominio solo se habilita cuando el cliente se detecta correctamente.

> **Nota:**
>
> Si un usuario prefiere el cliente HTML5 o el administrador lo exige, el método de autenticación PassThrough de dominio no está habilitado.

Al iniciar la URL de StoreFront en un explorador, se muestra el aviso **Detectar Receiver**.

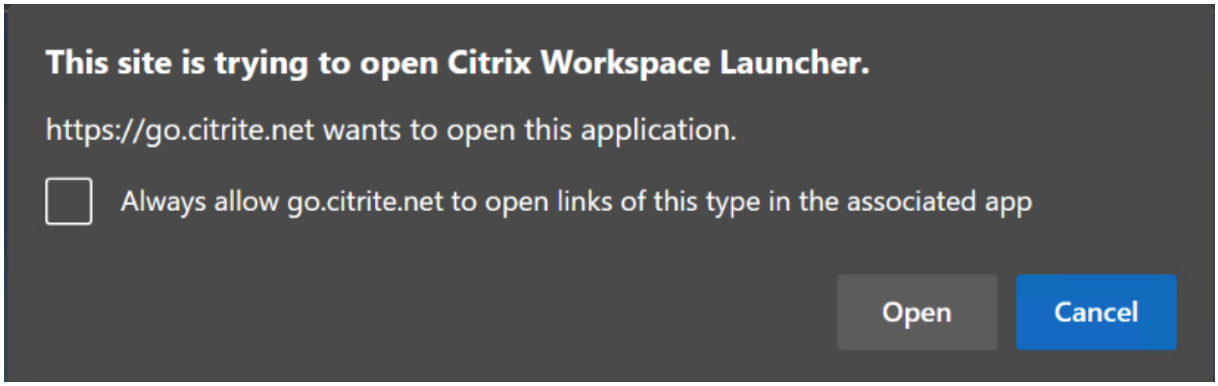
Si los dispositivos están administrados, configure la directiva de grupo para inhabilitar este aviso, en lugar de inhabilitar la detección de clientes. Para obtener más información, consulte:

- URLAllowlist en la documentación de Microsoft.
- URLAllowlist en la documentación de Google Chrome.

> **Nota:**
>
> El controlador de protocolo utilizado por la aplicación Workspace es **receiver:**. Configúrelo como una de las URL permitidas.

Los usuarios también pueden seleccionar la casilla de verificación, como se muestra en el siguiente aviso de ejemplo, para una URL de StoreFront en la solicitud de detección del cliente. Al seleccionar esta casilla de verificación, se evita también el aviso en inicios posteriores.




En los siguientes pasos se explica cómo configurar Citrix Gateway como IdP.

### Crear una directiva de IdP de OAuth en el dispositivo Citrix Gateway local

La creación de una directiva de autenticación de IdP de OAuth implica las siguientes tareas:

1. Crea un perfil de IdP de OAuth.
2. Agregar una directiva de IdP de OAuth.
3. Enlazar la directiva de IdP de OAuth a un servidor virtual.
4. Enlazar el certificado globalmente.

#### Crear un perfil de IdP de OAuth

1. Para crear un perfil de IdP de OAuth a través de la CLI, escriba lo siguiente en el símbolo del sistema:

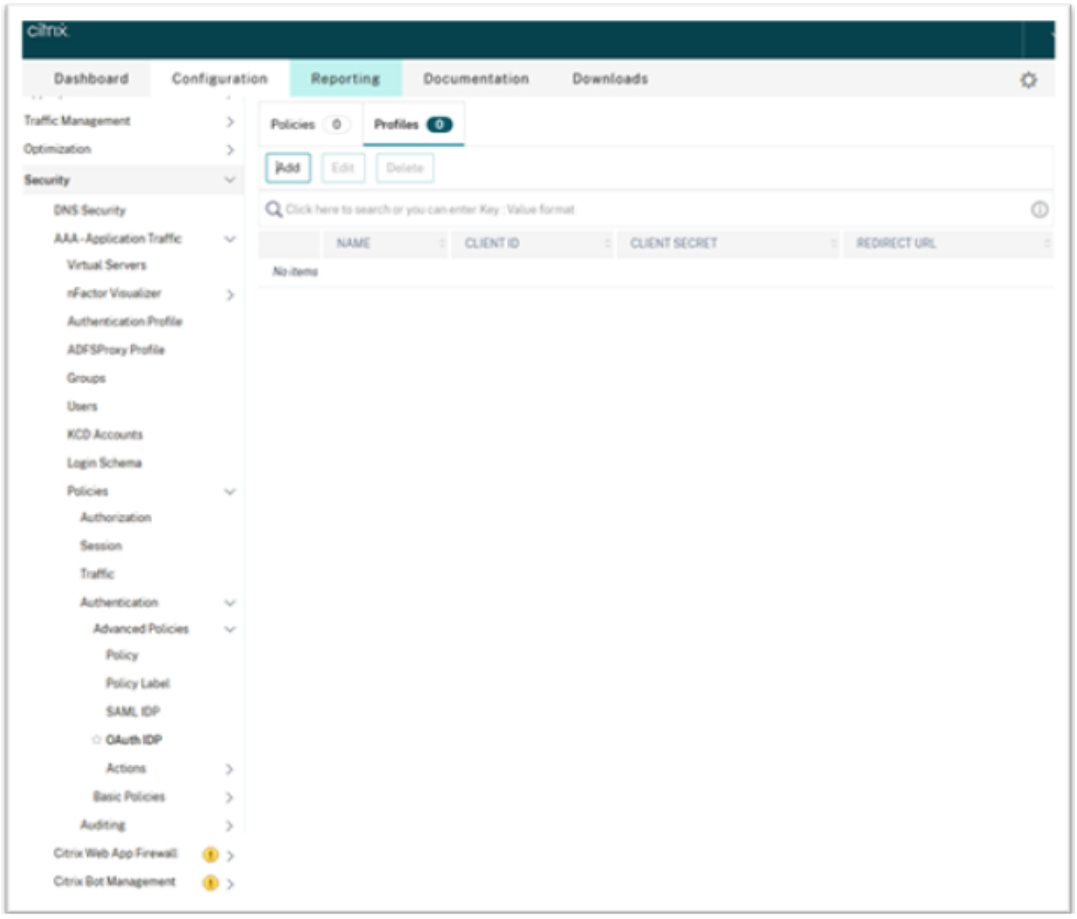
```
add authentication OAuthIdPProfile <name> [-clientID <string>][-
    clientSecret ][-redirectURL <URL>][-issuer <string>][-audience
    <string>][-skewTime <mins>] [-defaultAuthenticationGroup <
    string>]

add authentication OAuthIdPPolicy <name> -rule <expression> [-
    action <string> [-undefAction <string>] [-comment <string>][-
    logAction <string>]

add authentication ldapAction <name> -serverIP <IP> -ldapBase "dc=
    aaa,dc=local"

ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password
    > -ldapLoginName sAMAccountName

add authentication policy <name> -rule <expression> -action <
    string>

```

```
bind authentication vserver auth_vs -policy <ldap_policy_name> -
    priority <integer> -gotoPriorityExpression NEXT

bind authentication vserver auth_vs -policy <OAuthIdPPolicyName> -
    priority <integer> -gotoPriorityExpression END

bind vpn global  - certkey <>

<!--NeedCopy-->
```

2. Para crear un perfil de IdP de OAuth a través de la GUI:

   a) Inicie sesión en el portal de administración local de Citrix Gateway y vaya a **Security** > **AAA – Application Traffic** > **Policies** > **Authentication** > **Advanced Policies** > **OAuth IDP**.




   b) En la página **OAuth IdP**, haga clic en la ficha **Profiles** y, a continuación, en **Add**.

   c) Configure el perfil de IdP de OAuth.

> **Nota:**
>
> - Copie y pegue los valores de ID de cliente, secreto y URL de redireccionamiento

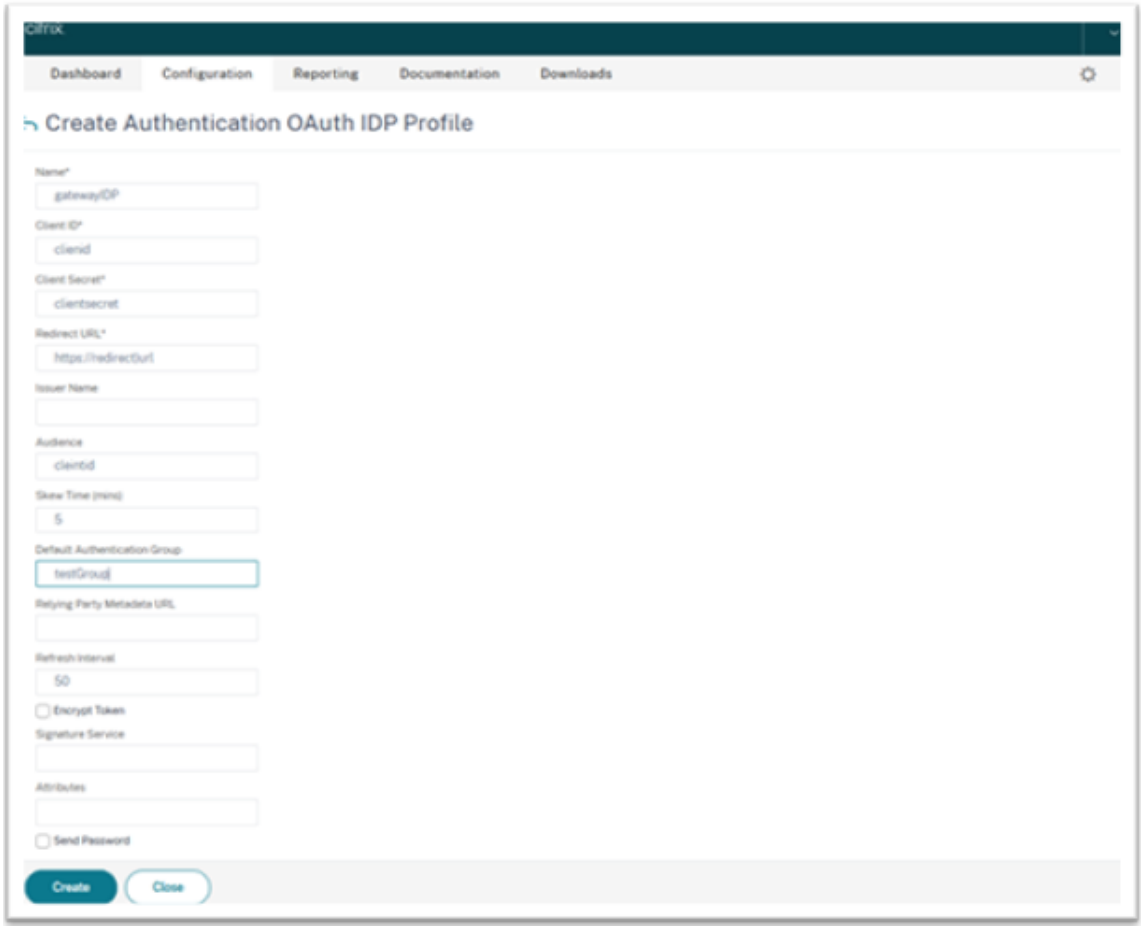
> desde la ficha **Citrix Cloud** > **Identity and Access Management** > **Identity and Access Management** para establecer la conexión con Citrix Cloud.
> - Introduzca la URL de Gateway correctamente en el campo **Issuer Name**. Por ejemplo: `https://GatewayFQDN.com`.
> - Copie y pegue también el ID de cliente en el campo **Audience**.
> - **Send Password**: Habilite esta opción para admitir Single Sign-On. De forma predeterminada, esta opción está inhabilitada.

d) En la pantalla **Create Authentication OAuth IdP Profile**, defina los valores para los siguientes parámetros y haga clic en **Create**.

- **Name**: Nombre del perfil de autenticación. Debe empezar por una letra, un número o un guion bajo (_). El nombre solo debe tener letras, números y guiones (-), punto (.), libra (#), espacio (), arroba (@), igual (=), dos puntos (:) y guiones bajos. No puede cambiar el nombre una vez creado el perfil.
- **Client ID**: Cadena única que identifica al proveedor de servicios. El servidor de autorización infiere la configuración del cliente mediante este ID. Longitud máxima: 127.
- **Client Secret**: Cadena secreta establecida por el usuario y el servidor de autorización. Longitud máxima: 239.
- **Redirect URL**: Dispositivo de punto final del proveedor de servicios al que se debe enviar el código/token.
- **Issuer Name**: Identidad del servidor cuyos tokens se van a aceptar. Longitud máxima: 127. Ejemplo: `https://GatewayFQDN.com`.
- **Audience**: Destinatario al que se dirige el token enviado por el IdP. El destinatario verifica este token.
- **Skew Time**: Esta opción especifica el sesgo de reloj (en minutos) que Citrix ADC permite para un token entrante. Por ejemplo, si skewTime es 10, el token es válido desde (hora actual - 10) minutos hasta (hora actual + 10) minutos, es decir, 20 minutos en total. Valor predeterminado: 5
- **Default Authentication Group**: Un grupo que se agrega a la lista de grupos internos de la sesión cuando el IdP elige este perfil y que se puede usar en el flujo nFactor. Se puede usar en la expresión (AAA.USER.IS_MEMBER_OF(“xxx”)) para que las directivas de autenticación identifiquen el flujo nFactor relacionado con el usuario de confianza. Longitud máxima: 63

Se agrega un grupo a la sesión de este perfil para simplificar la evaluación de las directivas y ayudar a personalizarlas. Este es el grupo predeterminado que se elige cuando la autenticación tiene éxito además de los grupos extraídos. Longitud máxima: 63.

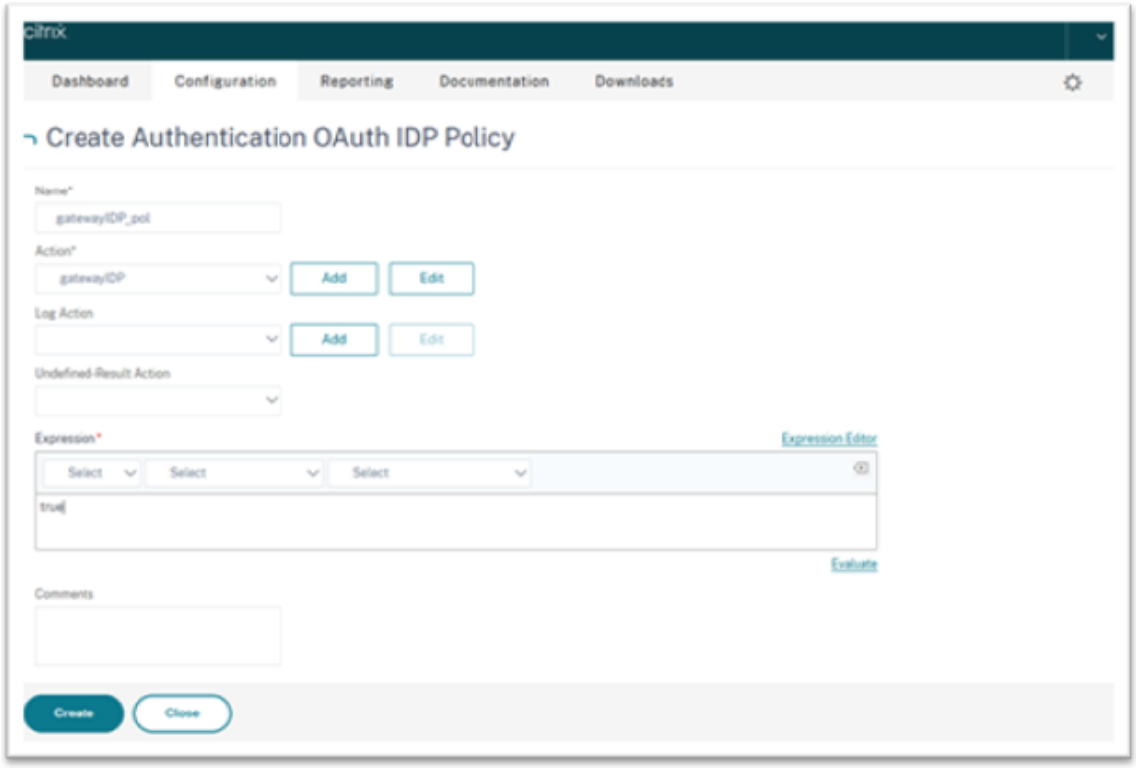
 




**Agregar una directiva de IdP de OAuth**

1. En la página OAuth IdP , haga clic en **Policies** y, a continuación, en **Add**.
2. En la pantalla **Create Authentication OAuth IdP Policy**, defina los valores de los siguientes parámetros y haga clic en **Create**.
   - **Name**: El nombre de la directiva de autenticación.
   - **Action**: Nombre del perfil creado anteriormente.
   - **Log Action**: Nombre de la acción del registro de mensajes que se utilizará cuando una solicitud coincida con esta directiva. No es un campo obligatorio.
   - **Undefined-Result Action**: Acción que realizar si el resultado de la evaluación de directivas es indefinido (UNDEF). No es un campo obligatorio.
   - **Expression**: Expresión sintáctica predeterminada que la directiva utiliza para responder a una solicitud específica. Por ejemplo, true.
   - **Comments**: Cualquier comentario sobre la directiva.




> **Nota:**
>
> Cuando sendPassword se establece en ON (tiene el valor OFF de forma predeterminada), las credenciales del usuario se cifran y se transmiten a través de un canal seguro a Citrix Cloud. La transmisión de las credenciales de usuario a través de un canal seguro le permite habilitar Single Sign-On en Citrix Virtual Apps and Desktops al iniciarse.

**Enlazar la directiva de OAuthIDP y la directiva de LDAP al servidor de autenticación virtual**

Ahora debe enlazar la directiva de IdP de OAuth al servidor de autenticación virtual en Citrix Gateway local.

1. Inicie sesión en el portal de administración local de Citrix Gateway y vaya a **Configuration** > **Security** > **AAA-Application Traffic** > **Policies** > **Authentication** > **Advanced Policies** > **Actions** > **LDAP**.
2. En la pantalla **LDAP Actions**, haga clic en **Add**.
3. En la pantalla c, defina los valores de los siguientes parámetros y haga clic en **Create**.
   - **Name**: El nombre de la acción LDAP.
   - **ServerName/ServerIP**: Proporcione el FQDN o la IP del servidor LDAP.
   - Elija valores apropiados para **Security Type**, **Port**, **Server Type** y **Time-Out**.
   - Asegúrese de que la opción **Authentication** esté marcada.
   - **Base DN**: Base desde la que se inicia la búsqueda LDAP. Por ejemplo `dc=aaa`, `dc=local`.

- **Administrator Bind DN**: Nombre de usuario del enlace al servidor LDAP. Por ejemplo: `admin@aaa.local`.
- **Administrator Password/Confirm Password**: Contraseña para enlazar LDAP.
- Haga clic en **Test Connection** para probar la configuración.
- **Server Logon Name Attribute**: Elija «sAMAccountName».
- Otros campos no son obligatorios y, por lo tanto, se pueden configurar según sea necesario.

4. Vaya a **Configuration** > **Security** > **AAA-Application Traffic** > **Policies** > **Authentication** > **Advanced Policies** > **Policy**.
5. En la pantalla **Authentication Policies**, haga clic en **Add**.
6. En la página **Create Authentication Policy**, defina los valores de los siguientes parámetros y haga clic en **Create**.

   - **Name**: Nombre de la directiva de autenticación de LDAP.
   - **Action Type**: Elija LDAP.
   - **Action**: Elija la acción LDAP.
   - **Expression**: Expresión sintáctica predeterminada que la directiva utiliza para responder a una solicitud específica. Por ejemplo, true**.

#### Enlazar el certificado globalmente a la VPN

Para enlazar el certificado de forma global a la VPN, se requiere acceso de CLI al dispositivo Citrix Gateway local. Con Putty (o similar), inicie sesión en el dispositivo Citrix Gateway local mediante SSH.

1. Inicie una utilidad de línea de comandos, como Putty.
2. Inicie sesión en Citrix Gateway local mediante SSH.
3. Escriba este comando:
   `show vpn global`

   > **Nota:**
   >
   > No se debe enlazar ningún certificado.

   Mostrar VPN global/en-us/citrix-workspace-app-for-windows/media/show-vpn-global.png
4. Para mostrar los certificados en el dispositivo Citrix Gateway local, escriba el siguiente comando:
   `show ssl certkey`
5. Seleccione el certificado apropiado y escriba el siguiente comando para enlazar el certificado de forma global a la VPN:

   `bind vpn global -certkey cert_key_name`

donde cert_key_name es el nombre del certificado.

6. Escriba el siguiente comando para comprobar si el certificado está enlazado globalmente a la VPN:

   ```
   show vpn global
   ```

   Mostrar VPN global/en-us/citrix-workspace-app-for-windows/media/show-vpn-global-1.png

## Configurar PassThrough de dominio como método de autenticación en Citrix Gateway

Cuando termine de configurar Citrix Gateway como IdP, siga estos pasos para configurar PassThrough de dominio como método de autenticación en Citrix Gateway.

Cuando se establece PassThrough de dominio como método de autenticación, el cliente utiliza tíquets de Kerberos, en lugar de credenciales, para autenticarse.
Citrix Gateway admite tanto suplantación como delegación limitada de Kerberos (KCD). Sin embargo, en este artículo se describe la autenticación KCD. Para obtener más información, consulte CTX236593.

La configuración de PassThrough de dominio incluye los siguientes pasos:

1. Configuración de delegación limitada de Kerberos
2. Configuración del cliente

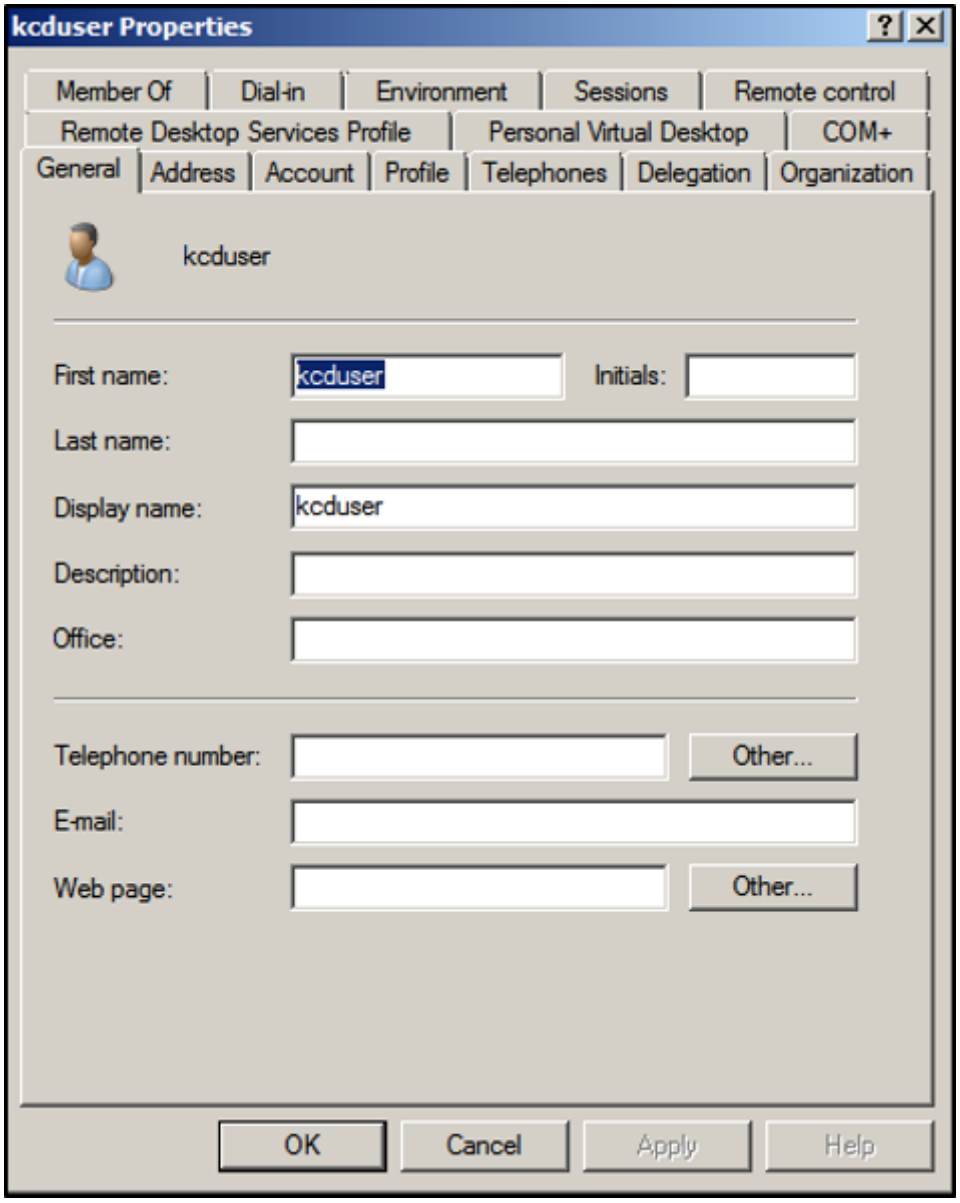
### Configuración de delegación limitada de Kerberos

1. Crear un usuario de KCD en Active Directory

   Kerberos funciona con un sistema de concesión de tíquets para autenticar a los usuarios en los recursos, e implica un cliente, un servidor y un centro de distribución de claves (KDC).

   Para que Kerberos funcione, el cliente debe solicitar un tíquet al KDC. El cliente primero debe autenticarse en el KDC con su nombre de usuario, contraseña y dominio antes de solicitar un tíquet, denominado solicitud AS.




2. Asocie al nuevo usuario con el nombre de principal de servicio (SPN).

   El cliente utiliza el SPN de Gateway para autenticarse.

   - Nombre principal de servicio (SPN): Un nombre principal de servicio (SPN) es un identificador único de una instancia de servicio. La autenticación Kerberos usa SPN para asociar una instancia de servicio a una cuenta de inicio de sesión de servicio. Esta función permite que una aplicación cliente solicite la autenticación de servicio de una cuenta, incluso si el cliente no tiene el nombre de la cuenta.

   SetSPN es la aplicación utilizada para administrar los SPN en un dispositivo Windows. Con SetSPN, se pueden ver, modificar y eliminar registros de SPN.

   a) En el servidor de Active Directory, abra un símbolo del sistema.

b) En el símbolo del sistema, introduzca el siguiente comando:

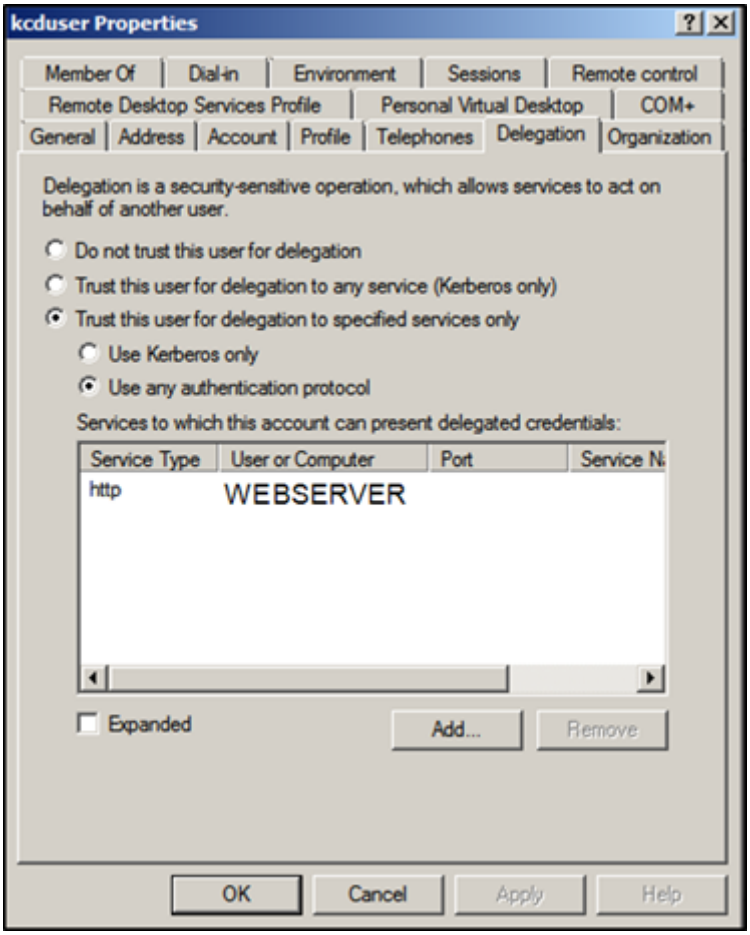
```
setspn -A http/<LB fqdn> <domain\Kerberos user>
```

c) Para confirmar los SPN del usuario de Kerberos, ejecute el siguiente comando:

```
setspn -l <Kerberos user>
```

La ficha Delegación aparece después de ejecutar el comando `setspn`.

d) Seleccione las opciones **Confiar en este usuario para la delegación solo a los servicios especificados** y **Usar cualquier protocolo de autenticación**. Agregue el servidor web y seleccione el servicio HTTP.

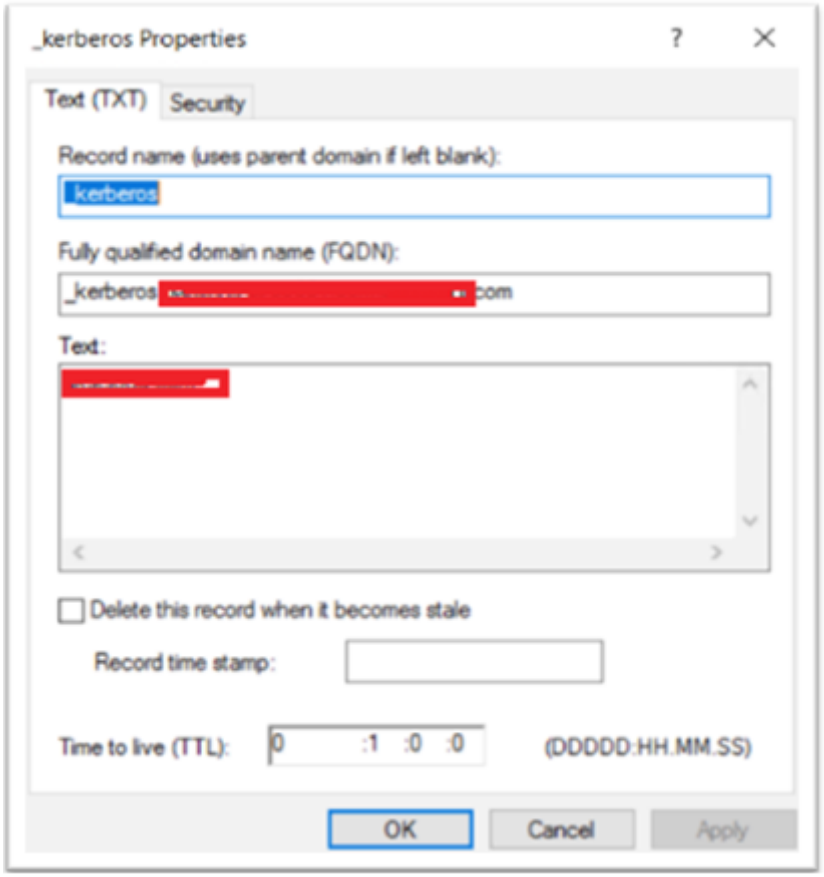



3. Cree un registro DNS para que el cliente encuentre el SPN de Gateway:

Agregue un registro TXT de DNS en Active Directory.

> **Nota:**
>
> El nombre debe comenzar por _Kerberos, los datos deben ser el nombre de dominio. El FQDN debe mostrar Kerberos..




El cliente unido al dominio de Windows usa _kerberos.fqdn para solicitar tíquets. Por ejemplo, si el cliente está unido a citrite.net, el sistema operativo puede obtener tíquets para cualquier sitio web con *.citrite.net. Sin embargo, si el dominio de Gateway es externo, como gateway.citrix.com, el sistema operativo cliente no puede obtener el tíquet de Kerberos.

Por lo tanto, debe crear un registro TXT de DNS que ayude al cliente a buscar _kerberos.gateway.citrix.com y obtener el tíquet de Kerberos para la autenticación.

4. Configure Kerberos como factor de autenticación.

   a) Cree una cuenta de KCD para el usuario de NetScaler. Aquí hemos optado por hacerlo manualmente, pero puede crear un archivo keytab.

   > **Nota:**
   >
   > Si utiliza dominios alternativos (dominio interno y dominio externo), debe configurar el SPN del servicio en HTTP/PublicFQDN.com@InternalDomain.ext

   - **Realm**: Territorio Kerberos. Por lo general, el sufijo del dominio interno.
   - **User Realm**: Es el sufijo del dominio interno del usuario.
   - **Enterprise Realm**: Solo se debe dar en ciertas implementaciones de KDC en las que KDC espera un nombre de usuario empresarial, en lugar de un nombre principal.

- **Delegated User**: Es la cuenta de usuario de NetScaler para KCD que creó en AD en los pasos anteriores. Asegúrese de que la contraseña es correcta.


b) Asegúrese de que el perfil de sesión utiliza la cuenta de KCD correcta. Enlace la directiva de sesión al servidor virtual de autenticación, autorización y auditoría.


c) Enlace la directiva de autenticación al servidor virtual de autenticación, autorización y auditoría. Estas directivas utilizan métodos de autenticación, autorización y auditoría que no obtienen una contraseña del cliente, de ahí la necesidad de usar KCD. Sin embargo, deben obtener el nombre de usuario y la información de dominio, en formato UPN.

> **Nota:**
>
> Puede usar el análisis de EPA o dirección IP para diferenciar los dispositivos unidos a

> un dominio y los que no están unidos a un dominio y usar Kerberos o LDAP normal como factor de autenticación.

**Configurar el cliente**

Para que Single Sign-On funcione correctamente en el VDA, haga lo siguiente.

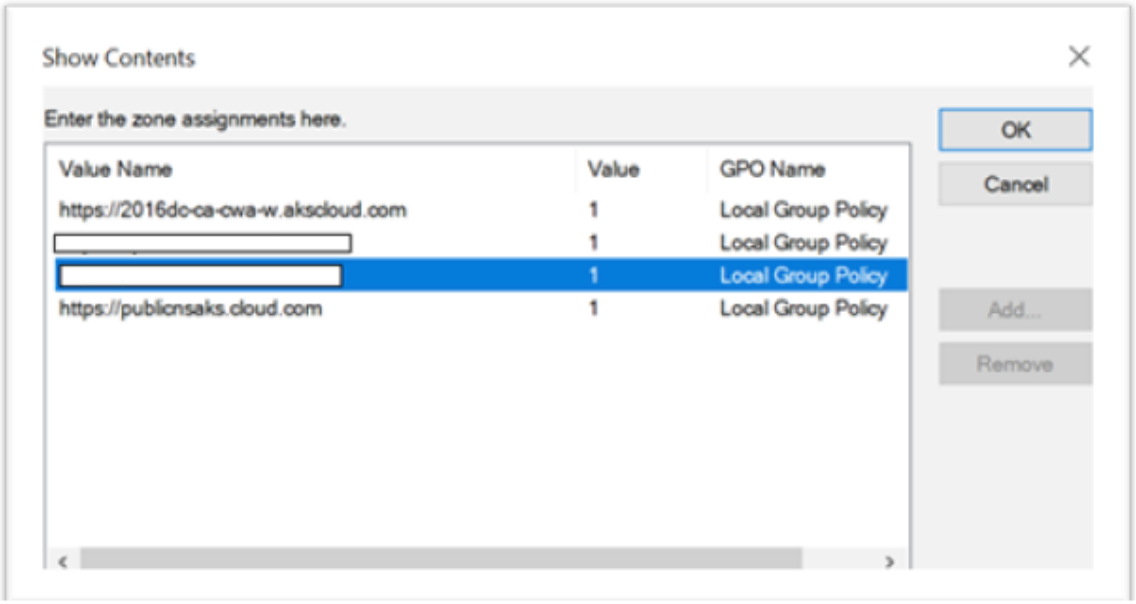
**Requisitos previos:**

- Máquina unida a un dominio
- Citrix Workspace 2112.1 o posterior con Single Sign-On habilitado
- URL de confianza necesarias que comprueban si las conexiones son seguras
- Validar Kerberos desde el cliente y AD. El sistema operativo del cliente debe tener conectividad con AD para obtener los tíquets de Kerberos.

A continuación, se presentan algunas de las URL de confianza en el explorador.

- FQDN o URL de Gateway
- FQDN de AD
- URL del espacio de trabajo para Single Sign-On con inicios desde un explorador.

1. Si utiliza Internet Explorer, Microsoft Edge o Google Chrome, haga lo siguiente:
    a) Inicie el explorador.
    b) Abra el Editor de directivas de grupo local en el cliente.




    a) Vaya a la página **Configuración del equipo** > **Componente de Windows** > **Internet Explorer**> **Panel de control de Internet** > **Seguridad**.
    b) Abra Lista de asignación de sitio a zona y agregue todas las URL enumeradas con el valor uno (1).

c) (Opcional) Ejecute `Gpupdate` para aplicar directivas.

2. Si utiliza el explorador Mozilla Firefox, haga lo siguiente:

a) Abra el explorador.

b) Escriba `about:config` en la barra de búsqueda.

c) Acepte el riesgo y continúe.

d) En el campo de búsqueda, escriba **negotiate**.

e) En la lista de datos completados, verifique si **network.negotiate-auth.trusted-uris** está configurado en el valor de dominio.


De esta forma, se completa la configuración en el lado del cliente.

3. Inicie sesión con la aplicación Workspace o con el explorador en Workspace.

Esto no debe solicitar el nombre de usuario ni la contraseña en un dispositivo unido a un dominio.

### Solución de problemas de Kerberos

> **Nota:**
>
> Para ejecutar este paso de verificación, debe ser administrador de dominio.

En el símbolo del sistema o en Windows PowerShell, ejecute el siguiente comando para comprobar la validación del tíquet de Kerberos para el usuario de SPN:

```
KLIST get host/FQDN of AD
```

## PassThrough de dominio a Citrix Workspace con Azure Active Directory como proveedor de identidades

January 18, 2023

Se puede implementar Single Sign-On (SSO) en Citrix Workspace con Azure Active Directory (AAD) como proveedor de identidades con dispositivos de punto final/VM unidos a un dominio, híbridos o inscritos en AAD.

Con esta configuración, también puede usar Windows Hello para SSO en Citrix Workspace mediante dispositivos de punto final inscritos en AAD.

- Puede autenticarse en la aplicación Citrix Workspace con Windows Hello.
- Autenticación basada en FIDO2 con la aplicación Citrix Workspace.
- Single Sign-On en la aplicación Citrix Workspace desde máquinas unidas a Microsoft AAD (AAD como IdP) y acceso condicional con AAD.

Para el inicio de sesión único (SSO) en aplicaciones y escritorios virtuales, puede implementar FAS o configurar la aplicación Citrix Workspace de la siguiente manera.

> **Nota:**
>
> SSO en los recursos de Citrix Workspace solo funciona con Windows Hello. Sin embargo, se le pedirá el nombre de usuario y la contraseña al acceder a sus aplicaciones y escritorios virtuales publicados. Para resolver este aviso, puede implementar FAS y SSO en escritorios y aplicaciones virtuales.

**Requisitos previos:**

1. Conecte Azure Active Directory a Citrix Cloud. Para obtener más información, consulte Conectar Azure Active Directory a Citrix Cloud en la documentación de Citrix Cloud.
2. Active la autenticación de Azure AD para acceder al espacio de trabajo Para obtener más información, consulte Habilitar la autenticación de Azure AD para espacios de trabajo en la documentación de Citrix Cloud.

Para implementar SSO en Citrix Workspace:

1. Configure la aplicación Citrix Workspace con includeSSON.
2. Inhabilite el atributo `prompt=login` en Citrix Cloud.
3. Configure PassThrough de Azure Active Directory con Azure Active Directory Connect.

### Configurar la aplicación Citrix Workspace para que admita SSO

**Requisitos previos:**

- Citrix Workspace 2109 o una versión posterior.

> **Nota:**
>
> Si usa FAS para SSO, no es necesaria la configuración de Citrix Workspace.

1. Instale la aplicación Citrix Workspace desde la línea de comandos de administración con la opción `includeSSON`:

   ```
   CitrixWorkspaceApp.exe /includeSSON
   ```

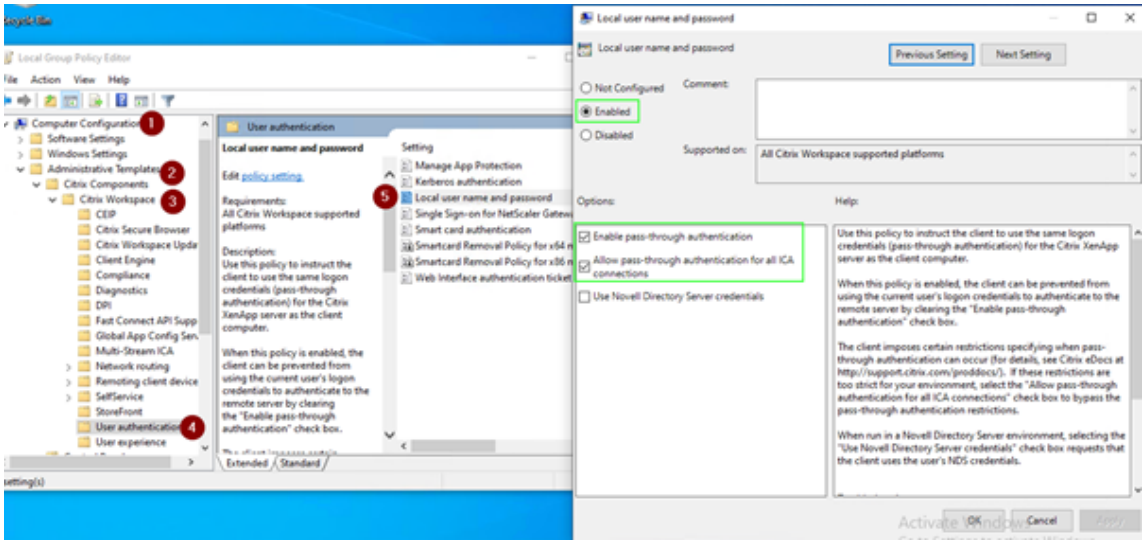
2. Cierre sesión en el cliente de Windows e inicie sesión para iniciar el servidor SSON.

3. Haga clic en **Configuración del equipo** > **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Autenticación de usuarios** para cambiar el GPO de Citrix Workspace y permitir **el nombre de usuario y la contraseña actuales**.

   > **Nota:**
   >
   > Estas directivas se pueden enviar al dispositivo cliente a través de Active Directory. Este paso solo es necesario para acceder a Citrix Workspace desde el explorador web.

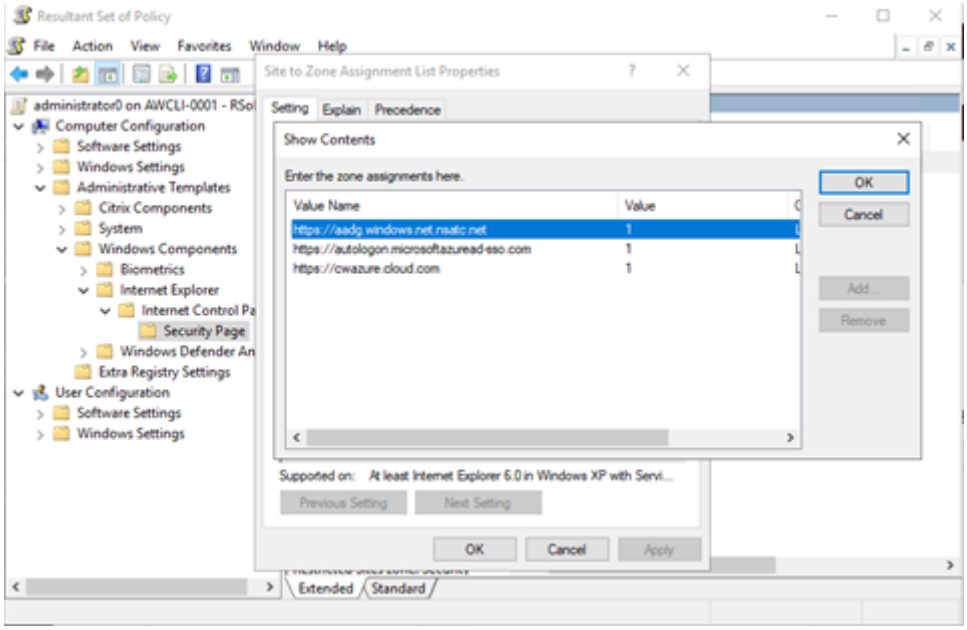
4. Habilite la configuración como se indica en la captura de pantalla.




5. Agregue los siguientes sitios de confianza a través del GPO:

   - `https://aadg.windows.net.nsatc.net`
   - `https://autologon.microsoftazuread-sso.com`
   - `https://xxxtenantxxx.cloud.com`: URL del espacio de trabajo



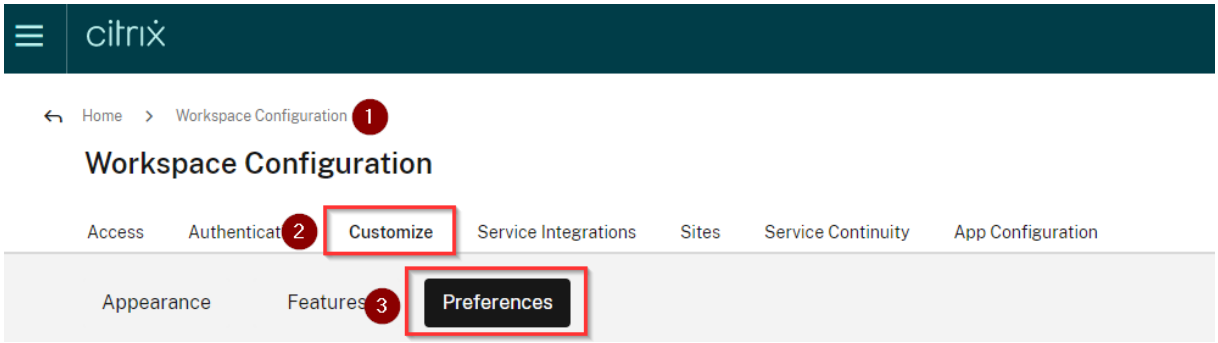

**Nota:**

Cuando el registro **AllowSSOForEdgeWebview** de `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle` se establece en false, se inhabilita Single Sign-On para AAD.

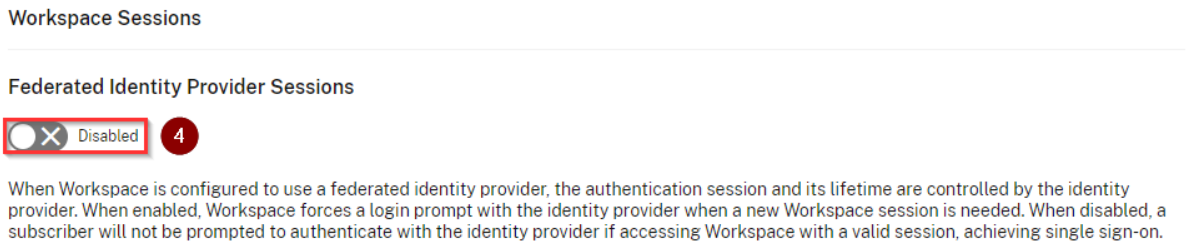
### Inhabilitar el parámetro prompt=login en Citrix Cloud

De forma predeterminada, `prompt=login` está habilitado para Citrix Workspace, lo que fuerza la autenticación incluso si el usuario optó por **mantener abierta la sesión** o si el dispositivo está unido a Azure AD.

Puede inhabilitar `prompt=login` en su cuenta de Citrix Cloud. Vaya a `Workspace Configuration\Customize\Preferences-Federated Identity Provider Sessions` e inhabilite la opción. Para obtener más información, consulte el artículo CTX253779 de Citrix Knowledge Center.






> **Nota:**
>
> En los dispositivos unidos a AAD o a AAD híbrido, si se utiliza AAD como IdP para Workspace, la aplicación Citrix Workspace no solicita las credenciales. Los usuarios pueden iniciar sesión automáticamente con una cuenta profesional o educativa.
>
> Para permitir que los usuarios inicien sesión con una cuenta diferente, establezca el siguiente registro en false.
>
> Cree y agregue una cadena de Registro REG_SZ con el nombre **AllowSSOForEdgeWebview** en `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle` o `Computer\HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle` y establezca su valor en False. Como alternativa, si los usuarios cierran sesión en la aplicación Citrix Workspace, podrán iniciar sesión con una cuenta diferente la próxima vez.

### Configurar PassThrough de Azure Active Directory con Azure Active Directory Connect

- Si va a instalar Azure Active Directory Connect por primera vez, en la página **User sign-in**, seleccione **Pass-through Authentication** como método de inicio de sesión. Para obtener más información, consulte Azure Active Directory Pass-Through Authentication: Quickstart en la documentación de Microsoft.
- Si ya tiene Microsoft Azure Active Directory Connect:
  1. Seleccione la tarea **Change user sign-in** y haga clic en **Next**.
  2. Seleccione **Pass-through Authentication** como método de inicio de sesión.

> **Nota:**
>
> Puede omitir este paso si el dispositivo cliente está unido a Azure AD o tiene una unión híbrida. Si el dispositivo está unido a AD, la autenticación PassThrough de dominio funciona mediante la autenticación Kerberos.

# PassThrough de dominio a Citrix Workspace con Okta como proveedor de identidades

January 18, 2023

Puede implementar Single Sign-On en Citrix Workspace con Okta como proveedor de identidades (IdP).

**Requisitos previos:**

- Citrix Cloud
  - Cloud Connectors

  **Nota:**
  Si es la primera vez que usa Citrix Cloud, defina una ubicación de recursos y configure los conectores. Se recomienda tener al menos dos Cloud Connectors implementados en entornos de producción. Para obtener información sobre la instalación de Citrix Cloud Connectors, consulte Instalar Cloud Connector.

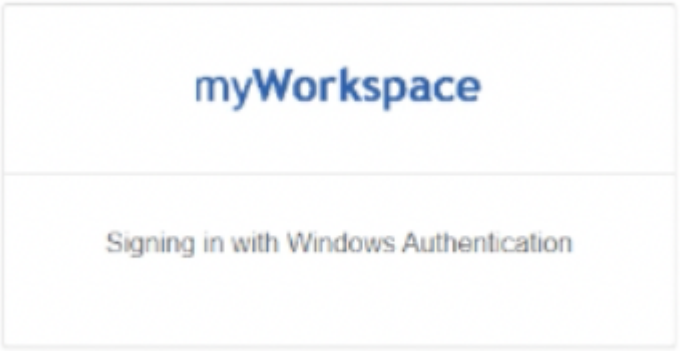
  - Citrix Workspace
  - Servicio de autenticación federada (opcional)
- Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service)
- VDA unido al dominio de AD o dispositivos físicos unidos a AD
- Arrendatario de Okta
  - Agente de IWA para Okta (autenticación integrada de Windows)
  - Okta Verify (Okta Verify se puede descargar de la tienda de aplicaciones) (opcional)
- Active Directory

1. Implemente el agente de AD para Okta:
   a) En el portal de administración de Okta, haga clic en **Directory** > **Directory Integrations**.
   b) Haga clic en **Add Directory** > **Add Active Directory**.
   c) Revise los requisitos de instalación siguiendo el flujo de trabajo, que cubre los requisitos de instalación y arquitectura del agente.
   d) Haga clic en el botón **Set Up Active Directory** y, a continuación, en **Download Agent**.
   e) Instale el agente de AD para Okta en un servidor Windows. Para ello, siga las instrucciones que se indican en Install the Okta Active Directory agent.

> **Nota:**
>
> Antes de instalar el agente, asegúrese de que se cumplen los requisitos previos mencionados en Active Directory integration prerequisites.

2. Configure la autenticación integrada de Windows (IWA):
   a) En el portal de administración de Okta, haga clic en **Security** y, a continuación, en **Delegated Authentication**
   b) En la página que se carga, desplácese a la sección **On-prem Desktop SSO** y haga clic en **Download Agent**.
   c) Configure las **reglas de redirección** para IWA. Para obtener más información, consulte Configure Identity Provider routing rules.
3. Inicie el portal de clientes de Okta.

   > **Nota:**
   >
   > - Cuando se instala el agente de IWA para Okta y el estado es habilitado, puede iniciar sesión desde un dispositivo unido a un dominio de Windows. Esta configuración además omite el inicio de sesión y lo dirige a la página de inicio de sesión de IWA y transmite las credenciales de usuario.
   >
   > 
   > 
   >
   > - Para obtener más información sobre cómo solucionar cualquier problema, consulte Install and configure the Okta IWA Web agent for Desktop single sign-on.
4. Inicie sesión en Citrix Cloud, en `https://citrix.cloud.com`, y habilite Okta como proveedor de identidades. Para obtener información, consulte Tech Insight: Authentication - Okta en la documentación de Citrix Tech Zone.

   > **Nota:**
   >
   > Puede iniciar sesión desde la aplicación Citrix Workspace o el explorador; ambos ofrecen la modalidad PassThrough que se indica en la documentación de Tech Zone.
5. Para el inicio de sesión único (SSO) en aplicaciones y escritorios virtuales, puede implementar FAS o configurar la aplicación Citrix Workspace.

> **Nota:**
>
> Sin FAS, se le pedirán el nombre de usuario y la contraseña de AD. Para obtener información sobre cómo habilitar FAS, consulte la sección "Habilite el Servicio de autenticación federada" en Configurar Single Sign-On en la aplicación Workspace.
> Si no usa FAS, configure la aplicación Citrix Workspace para que admita SSO.

## Proteger comunicaciones

April 6, 2023

Para proteger la comunicación entre el servidor Citrix Virtual Apps and Desktops y la aplicación Citrix Workspace, se pueden integrar las conexiones de la aplicación Citrix Workspace a través de todo un abanico de tecnologías de seguridad, como, por ejemplo:

- Citrix Gateway: Para obtener información, consulte los temas de esta sección, además de la documentación de Citrix Gateway y StoreFront.
- Un firewall: Los firewall o servidores de seguridad de red pueden permitir o bloquear los paquetes basándose en la dirección y el puerto de destino.
- Se admite desde la versión 1.0 hasta la versión 1.2 de Transport Layer Security (TLS).
- Servidor de confianza para establecer relaciones de confianza en las conexiones de la aplicación Citrix Workspace.
- ICA File Signing
- Protección de la autoridad de seguridad local (LSA)
- Solo para el servidor proxy de implementaciones de Citrix Virtual Apps: un servidor proxy SOCKS o un servidor proxy seguro. Los servidores proxy ayudan a limitar el acceso entrante y saliente de la red. También gestionan las conexiones entre la aplicación Citrix Workspace y el servidor. La aplicación Citrix Workspace admite protocolos de proxy seguro y SOCKS.
- Proxy saliente

### Citrix Gateway

Citrix Gateway (anteriormente Access Gateway) protege las conexiones a los almacenes de StoreFront. Además, permite a los administradores controlar de manera detallada el acceso de los usuarios a los escritorios y las aplicaciones.

Para conectarse a escritorios y aplicaciones a través de Citrix Gateway:

1. Especifique la URL de Citrix Gateway que el administrador proporciona de una de las siguientes maneras:

- La primera vez que use la interfaz de usuario de autoservicio, se le solicitará que introduzca la dirección URL en el cuadro de diálogo **Agregar cuenta**
- Cuando utilice más tarde la interfaz de usuario de autoservicio, puede introducir la URL en **Preferencias** > **Cuentas** > **Agregar**.
- Si quiere establecer una conexión mediante el comando storebrowse, escriba la dirección URL en la línea de comandos.

La dirección URL especifica la puerta de enlace y, si quiere, un almacén concreto:

- Para conectarse al primer almacén que encuentra la aplicación Citrix Workspace, use una URL en este formato:
  - https://puertadeenlace.empresa.com
- Para conectarse a un almacén específico, use una URL con este formato. Por ejemplo: https://puertadeenlace.empresa.com?. Esta dirección URL dinámica no tiene el formato estándar; no incluya = (el signo igual) en la URL. Si quiere establecer una conexión a un almacén concreto mediante storebrowse, puede que se necesiten comillas alrededor de la dirección URL en el comando storebrowse.

1. Cuando se le solicite, conéctese al almacén (a través de la puerta de enlace) con su nombre de usuario, contraseña y token de seguridad. Para obtener más información sobre este paso, consulte la documentación de Citrix Gateway.

Una vez completado el proceso de autenticación, se muestran los escritorios y las aplicaciones.

## Conectarse a través de un firewall

Los firewall o servidores de seguridad de red pueden permitir o bloquear los paquetes basándose en la dirección y el puerto de destino. Si utiliza un firewall, la aplicación Citrix Workspace para Windows puede comunicarse a través de él con el servidor web y el servidor de Citrix.

### Puertos comunes de comunicación Citrix

| Origen | Tipo | Puerto | Detalles |
|---|---|---|---|
| Aplicación Citrix Workspace | TCP | 80/443 | Comunicación con StoreFront |
| ICA o HDX | TCP/UDP | 1494 | Acceso a aplicaciones y escritorios virtuales |
| ICA o HDX con fiabilidad de la sesión | TCP/UDP | 2598 | Acceso a aplicaciones y escritorios virtuales |

| Origen | Tipo | Puerto | Detalles |
|---|---|---|---|
| ICA o HDX por TLS | TCP/UDP | 443 | Acceso a aplicaciones y escritorios virtuales |

Para obtener más información sobre los puertos, consulte el artículo CTX101810 de Citrix Knowledge Center.

### Transport Layer Security

Transport Layer Security (TLS) es el reemplazo del protocolo SSL (Secure Sockets Layer). La organización Internet Engineering Taskforce (IETF) le cambió el nombre a TLS al asumir la responsabilidad del desarrollo de TLS como un estándar abierto.

TLS protege las comunicaciones de datos mediante la autenticación del servidor, el cifrado del flujo de datos y la comprobación de la integridad de los mensajes. Algunas organizaciones, entre las que se encuentran organizaciones del gobierno de los EE. UU., requieren el uso de TLS para proteger las comunicaciones de datos. Es posible que estas organizaciones también exijan el uso de cifrado validado, como FIPS 140 (Federal Information Processing Standard). FIPS 140 es un estándar para cifrado.

Para utilizar el cifrado TLS como medio de comunicación, debe configurar el dispositivo de usuario y la aplicación Citrix Workspace. Para obtener información sobre cómo proteger las comunicaciones de StoreFront, consulte la sección Proteger de la documentación de StoreFront. Para obtener información sobre cómo proteger los VDA, consulte Transport Layer Security (TLS) en la documentación de Citrix Virtual Apps and Desktops.

Puede usar estas directivas para:

- Exigir el uso de TLS: Se recomienda usar TLS para las conexiones a través de redes que no son de confianza, incluido Internet.
- Exigir el uso de FIPS (Federal Information Processing Standards): Criptografía aprobada y seguir las recomendaciones de NIST SP 800-52. Estas opciones están inhabilitadas de forma predeterminada.
- Exigir el uso de una versión específica de TLS y de conjuntos de cifrado TLS específicos. Citrix admite los protocolos TLS 1.0, TLS 1.1 y TLS 1.2.
- Conectarse solamente a servidores específicos.
- Comprobar si el certificado del servidor se ha revocado.
- Comprobar si existe alguna directiva de emisión de certificados de servidor específica.
- Seleccionar un certificado de cliente concreto, si el servidor está configurado para solicitar uno.

**Importante:**
Estos conjuntos de cifrado se han retirado para mejorar la seguridad:

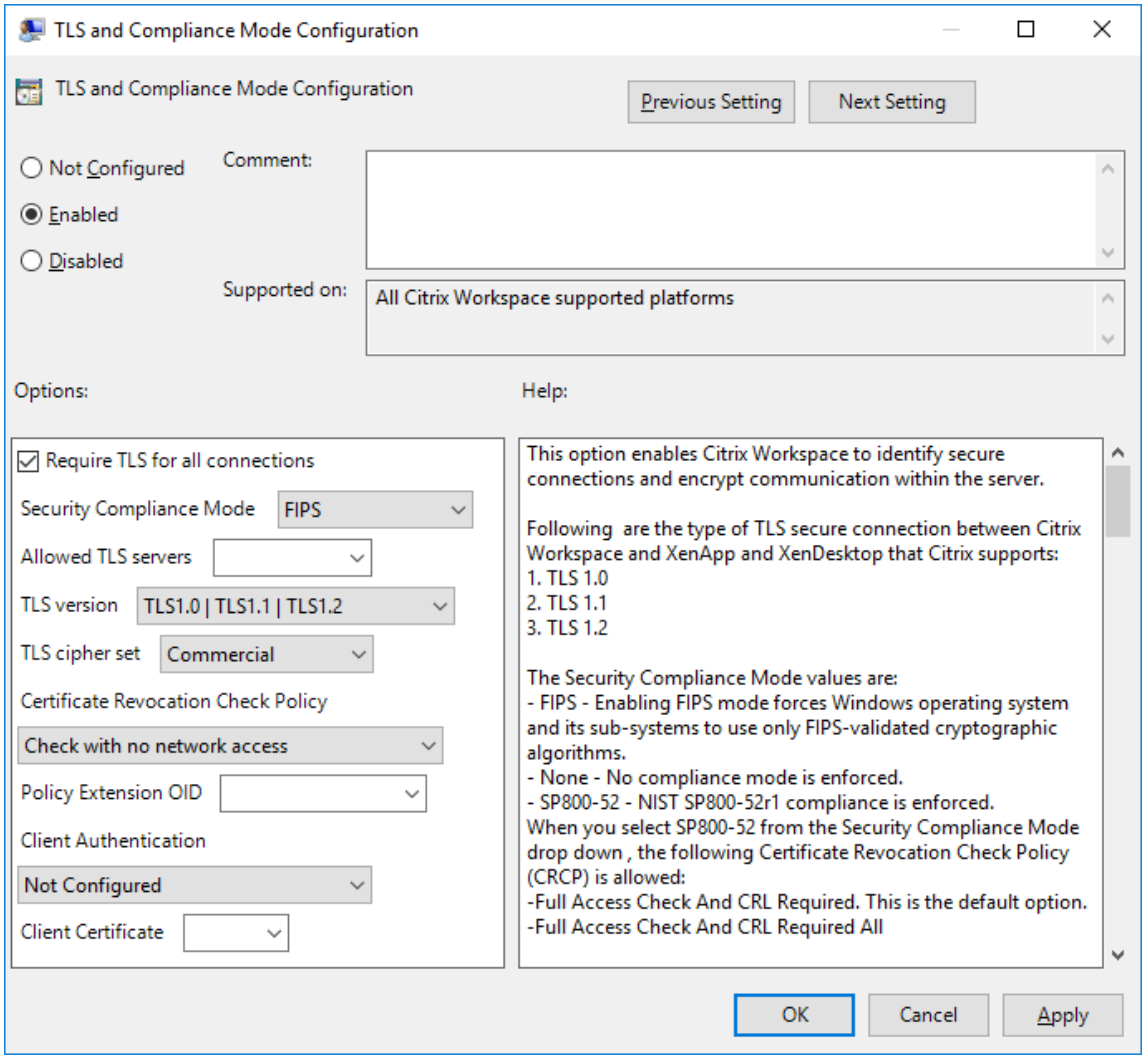
- Conjuntos de cifrado RC4 y 3DES
- Conjuntos de cifrado con el prefijo “TLS_RSA_*”
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- TLS_RSA_WITH_RC4_128_SHA (0x0005)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

Para obtener información sobre los conjuntos de cifrado admitidos, consulte el artículo CTX250104de Citrix Knowledge Center.

**Compatibilidad con TLS**

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Citrix Workspace** > **Redirección de red** y seleccione la directiva **Configuración del modo de conformidad y TLS**.




3. Seleccione **Habilitada** para habilitar las conexiones seguras y para cifrar la comunicación en el servidor. Configure estas opciones:

> **Nota:**
>
> Citrix recomienda usar TLS para proteger las conexiones.

   a) Seleccione **Requerir TLS para todas las conexiones** si quiere obligar a la aplicación Citrix Workspace a usar TLS en las conexiones con aplicaciones y escritorios publicados.

   b) En el menú **Modo de conformidad para la seguridad**, seleccione la opción correspondiente:

      i. **Ninguno:** No se impone ningún modo de conformidad.
      ii. **SP800-52**: Seleccione **SP800-52** para la conformidad con NIST SP 800-52. Seleccione esta opción solo si los servidores o la puerta de enlace cumplen las recomendaciones de NIST SP 800-52.

> **Nota:**
>
> Si selecciona **SP800-52**, se usará automáticamente la criptografía aprobada por FIPS, incluso aunque no esté seleccionada la opción **Habilitar FIPS**. Asimismo, habilite la opción de seguridad de Windows **Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash**. De lo contrario, la aplicación Citrix Workspace puede fallar al intentar conectarse a aplicaciones y escritorios publicados.

Si selecciona **SP800-52**, establezca la configuración de la directiva **Comprobación de revocación de certificados** en **Requerir comprobación con acceso completo y lista de revocación de certificados**.

Cuando selecciona **SP 800-52**, la aplicación Citrix Workspace verifica si el certificado de servidor sigue las recomendaciones de NIST SP 800-52. Si el certificado de servidor no las cumple, la aplicación Citrix Workspace no se podrá conectar.

i. **Habilitar FIPS**: Seleccione esta opción para exigir el uso de la criptografía aprobada por FIPS. Igualmente, habilite la opción de seguridad de Windows **Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash** en la directiva de grupo del sistema operativo. De lo contrario, la aplicación Citrix Workspace puede fallar al intentar conectarse a aplicaciones y escritorios publicados.

c) En el menú desplegable **Servidores TLS permitidos**, seleccione el número de puerto. Utilice una lista separada por comas para asegurarse de que la aplicación Workspace solo se conecta a un servidor especificado. Se pueden especificar comodines y números de puerto. Por ejemplo, *.citrix.com: 4433 permite la conexión a un servidor cuyo nombre común termine en .citrix.com en el puerto 4433. La precisión de la información que contenga un certificado de seguridad es responsabilidad del emisor del certificado. Si Citrix Workspace no reconoce o no confía en el emisor de un certificado, se rechaza la conexión.

d) En el menú **Versión de TLS**, seleccione una de las siguientes opciones:

- **TLS 1.0, TLS 1.1 o TLS 1.2:** Este es el parámetro predeterminado. Esta opción solo se recomienda si es un requisito del negocio usar TLS 1.0 para la compatibilidad.
- **TLS 1.1 o TLS 1.2**: Use esta opción para que las conexiones usen TLS 1.1 o TLS 1.2.
- **TLS 1.2:** Esta opción se recomienda si TLS 1.2 es un requisito del negocio.

a) **Conjunto de cifrado TLS**: Para obligar el uso de un conjunto de cifrado TLS específico, seleccione Gubernamental (GOV), Comercial (COM) o Todos (ALL). Para obtener más información, consulte el artículo CTX250104 de Citrix Knowledge Center.

b) En el menú **Directiva de comprobación de revocación de certificados**, seleccione alguna de las siguientes opciones:

- **Comprobar sin acceso a red**: Se lleva a cabo una comprobación de la lista de revocación de certificados. Solo se usan almacenes locales de listas de revocación de certificados. Se ignoran todos los puntos de distribución. Una comprobación de la lista de revocación de certificados que verifica el certificado del servidor disponible en el servidor de traspaso SSL o de Citrix Secure Web Gateway de destino no es obligatorio.
- **Comprobar con acceso completo:** Se lleva a cabo una comprobación de la lista de revocación de certificados. Se utilizan los almacenes locales de listas de revocación de certificados y todos los puntos de distribución. Si se encuentra información de revocación de un certificado, se rechaza la conexión. La comprobación de la lista de revocación de certificados para verificar el certificado de servidor disponible en el servidor de destino no es esencial.
- **Requerir comprobación con acceso completo y lista de revocación de certificados:** Se hace una comprobación de listas de revocación de certificados, a excepción de la entidad de certificación (CA) raíz. Se utilizan los almacenes locales de listas de revocación de certificados y todos los puntos de distribución. Si se encuentra información de revocación de un certificado, se rechaza la conexión. Para la verificación, es necesario encontrar todas las listas de revocación de certificados requeridas.
- **Requerir comprobación con acceso completo y todas las listas de revocación de certificados**: Se hace una comprobación de listas de revocación de certificados, incluida la entidad de certificación (CA) raíz. Se utilizan los almacenes locales de listas de revocación de certificados y todos los puntos de distribución. Si se encuentra información de revocación de un certificado, se rechaza la conexión. Para la verificación, es necesario encontrar todas las listas de revocación de certificados requeridas.
- **No comprobar:** No se comprueban listas de revocación de certificados.

a) Puede restringir la aplicación Citrix Workspace para que solo pueda conectarse a servidores con una directiva de emisión de certificados concreta, mediante un **OID de extensión de directiva**. Cuando se selecciona **OID de extensión de directiva**, la aplicación Citrix Workspace solamente acepta certificados de servidor que contienen ese OID de extensión de directiva.

b) En el menú **Autenticación del cliente**, seleccione alguna de las siguientes opciones:

- **Inhabilitada:** La autenticación de cliente está inhabilitada.
- **Mostrar selector de certificados:** Pedir siempre al usuario que seleccione un certificado.
- **Seleccionar automáticamente, si es posible:** Pedir al usuario que seleccione un certificado solo si hay varios para elegir.
- **No configurado**: La autenticación del cliente no está configurada.

- **Usar un certificado especificado:** Usar el certificado de cliente que esté definido en la opción "Certificado del cliente".

a) Use el parámetro **Certificado del cliente** para especificar la huella digital del certificado de identificación y evitar tener que preguntar al usuario innecesariamente.

b) Haga clic en **Aplicar** y **Aceptar** para guardar la directiva.

Para obtener información sobre la tabla de conexiones de red internas y externas, consulte el artículo CTX250104 de Citrix Knowledge Center.

## Servidor de confianza

### Aplicar conexiones de servidor de confianza

La directiva de configuración "Servidor de confianza" identifica y aplica relaciones de confianza en las conexiones de la aplicación Citrix Workspace.

Con esta directiva, los administradores pueden controlar cómo el cliente identifica la aplicación o el escritorio publicados a los que se conecta. El cliente determina un nivel de confianza, denominado región de confianza, con una conexión. La región de confianza, a su vez, determina cómo se configura el cliente para la conexión.

Al habilitar esta directiva, se evitan conexiones a los servidores que no se encuentran en las regiones de confianza.

De manera predeterminada, la identificación de la región se basa en la dirección del servidor con el que se conecta el cliente. Para ser miembro de la región de confianza, el servidor debe ser miembro de la **zona de Sitios de confianza** de Windows. Esto se puede configurar con el parámetro **Zona de Internet de Windows**.

También se puede confiar específicamente en la dirección del servidor mediante el parámetro **Address**. La dirección del servidor debe ser una lista de servidores separados por comas que admitan el uso de comodines. Por ejemplo, `cps*.citrix.com`.

Para habilitar la configuración de servidor de confianza mediante la plantilla administrativa de objetos de directiva de grupo

**Requisito previo:**

Debe salir de los componentes de la aplicación Citrix Workspace, incluida la Central de conexiones.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Redirección de red** > **Configuración de servidores de confianza**.
3. Marque **Habilitado** para obligar a que la aplicación Citrix Workspace identifique la región.

4. Marque **Aplicar configuración de servidor de confianza**. Esta opción obliga al cliente a realizar la identificación mediante un servidor de confianza.
5. Desde el menú desplegable **Zona de Internet de Windows**, seleccione la dirección del servidor de cliente. Esta configuración solo se aplica a la zona "Sitios de confianza" de Windows.
6. En el campo **Dirección**, establezca la dirección del servidor de cliente en una zona "Sitios de confianza" que no sea Windows. Puede utilizar una lista separada por comas.
7. Haga clic en **Aceptar** y **Aplicar**.

Cuando esta directiva está habilitada y el servidor no está en la región de confianza, se impide la conexión y se muestra un mensaje de error.
El servidor identificado debe agregarse a la **zona de Sitios de confianza** de Windows para que la conexión se realice correctamente. Por ejemplo, agregue el servidor como "http://" o "https://" para las conexiones SSL.

> **Nota:**
>
> Para las conexiones SSL, el nombre común del certificado debe ser de confianza. Para las conexiones que no son SSL, es necesario que todos los servidores contactados sean de confianza individualmente.

Además, debe asegurarse de que el FQDN interno de StoreFront se agregue a la zona de Intranet local o a las zonas de Sitios de confianza. Para obtener información, consulte **Modificar los parámetros de Internet Explorer** en la sección Autenticación.

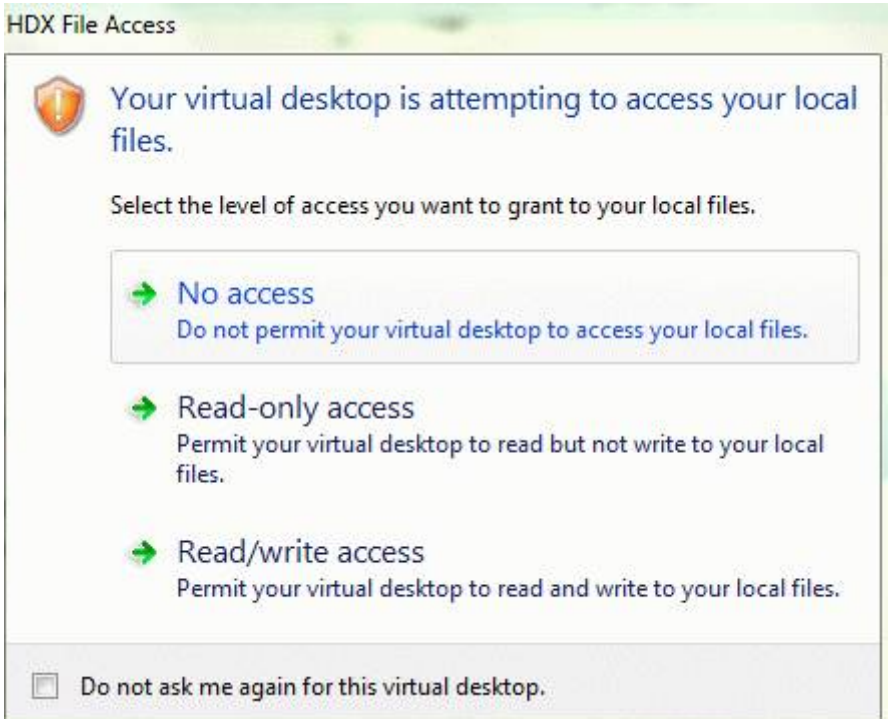
#### Confianza selectiva de clientes

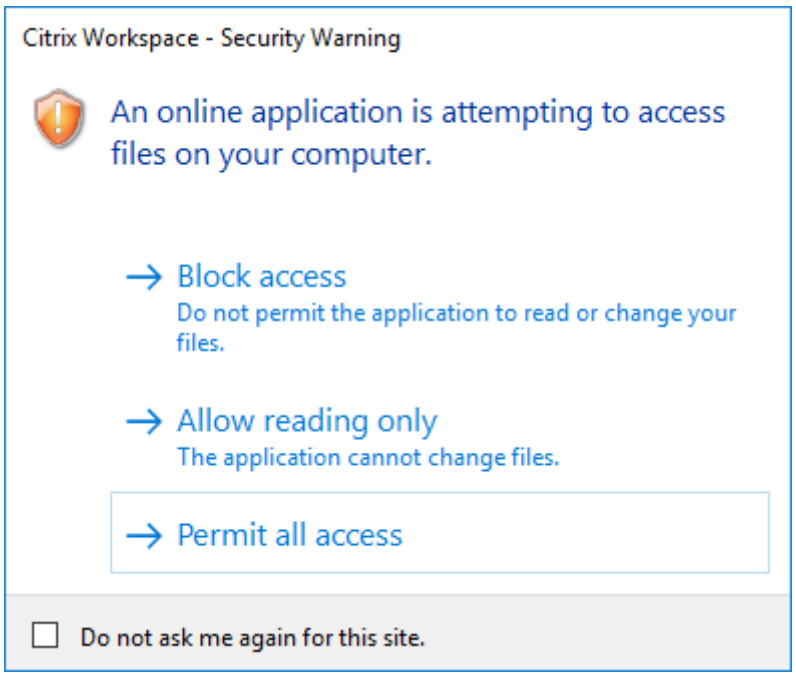
Además de permitir o impedir conexiones a los servidores, el cliente también utiliza las regiones para identificar el acceso SSO a archivos, micrófonos o cámaras web.

| Regiones | Recursos | Nivel de acceso |
|---|---|---|
| Internet | Archivo, micrófono, web | Solicitar acceso al usuario, no se permite SSO |
| Intranet | Micrófono, web | Solicitar acceso al usuario, se permite SSO |
| Sitios restringidos | Todas | Es posible que no se impida el acceso ni la conexión |
| De confianza | Micrófono, web | Lectura o escritura, se permite SSO |

Cuando el usuario ha seleccionado el valor predeterminado para una región, es posible que aparezca este cuadro de diálogo:




Los administradores pueden modificar este comportamiento predeterminado al crear y configurar las claves del Registro de la **confianza selectiva de cliente** mediante la directiva de grupo o en el Registro. Para obtener más información sobre cómo configurar las claves del Registro de la confianza selectiva de cliente, consulte el artículo CTX133565 de Knowledge Center.

### ICA File Signing

La función ICA File Signing (firma de archivos ICA) permite protegerse ante inicios no autorizados de escritorios y aplicaciones. La aplicación Citrix Workspace verifica si el inicio de la aplicación o del escritorio fue generado desde una fuente de confianza, basándose en una directiva de administración, y protege al usuario frente a inicios originados en servidores que no son de confianza. Puede configurar ICA File Signing mediante la plantilla administrativa de objetos de directiva de grupo o StoreFront. La función de firma de archivos ICA no está habilitada de forma predeterminada.

Para obtener información sobre cómo habilitar ICA File Signing para StoreFront, consulte Habilitar ICA File Signing en la documentación de StoreFront.

#### Configurar la firma del archivo ICA

> **Nota:**
>
> Si no se agrega CitrixBase.admx\adml al objeto de directiva de grupo (GPO) local, la directiva **Habilitar ICA File Signing** puede no estar presente.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix**.

3. Seleccione la directiva **Habilitar ICA File Signing** y seleccione una de las opciones según sea necesario:
    a) Habilitada: Indica que puede agregar el sello del certificado con firma a la lista de sellos de certificados de confianza permitidos.
    b) Certificados de confianza: Haga clic en **Mostrar** para quitar el sello del certificado con firma existente en la lista de permitidos. Puede copiar y pegar los sellos de certificados con firma desde las propiedades de los certificados.
    c) Directiva de seguridad: Seleccione una de las siguientes opciones en el menú.
        i. Permitir inicios con firma solamente (más seguro): Permite los inicios de solamente escritorios o aplicaciones con firma desde servidores de confianza. Aparece una advertencia de seguridad en caso de una firma no válida. No se puede iniciar la sesión por la falta de autorización.
        ii. Preguntar al usuario en inicios sin firma (menos seguro): Aparece un mensaje cuando se inicia una sesión sin firma o sin firma válida. Puede optar por continuar el inicio o cancelarlo (opción predeterminada).
4. Haga clic en **Aplicar** y **Aceptar** para guardar la directiva.
5. Reinicie la sesión de la aplicación Citrix Workspace para que los cambios surtan efecto.

**Para seleccionar y distribuir un certificado de firma digital:**

Al seleccionar un certificado de firma digital, recomendamos elegirlo a partir de esta lista de prioridades:

1. Adquiera un certificado con firma de código o un certificado con firma SSL a partir de una entidad de certificados (CA) pública.
2. Si su empresa dispone de una entidad de certificados privada, cree un certificado con firma de código o un certificado con firma SSL a través de la entidad de certificados privada.
3. Utilice un certificado SSL existente.
4. Cree un certificado raíz y distribúyalo a los dispositivos de usuario mediante un objeto de directiva de grupo o una instalación manual.

### Protección de la autoridad de seguridad local (LSA)

La aplicación Citrix Workspace ofrece la protección de la autoridad de seguridad local (LSA) de Windows, que conserva información sobre todos los aspectos de la seguridad local de un sistema. Esto proporciona el nivel LSA de protección del sistema para los escritorios alojados.

### Conectarse a través de un servidor proxy

Se usan servidores proxy para limitar el acceso hacia y desde la red, así como para administrar las conexiones entre los servidores y la aplicación Citrix Workspace para Windows. La aplicación Citrix Workspace admite protocolos de proxy seguro y SOCKS.

En la comunicación con el servidor, la aplicación Citrix Workspace utiliza los parámetros del servidor proxy configurados de forma remota en el servidor con Workspace para Web.

En la comunicación con el servidor web, la aplicación Citrix Workspace utiliza los parámetros de servidor proxy configurados a través de la opción **Internet** del explorador web predeterminado en el dispositivo de usuario. Configure los parámetros de **Internet** del explorador web predeterminado en el dispositivo de usuario según corresponda.

Para aplicar los parámetros de proxy a través del archivo ICA en StoreFront, consulte el artículo CTX136516de Citrix Knowledge Center.

### Compatibilidad con proxies salientes

SmartControl permite a los administradores configurar y aplicar directivas que afectan al entorno. Por ejemplo, es posible que quiera prohibir a los usuarios asignar unidades a sus escritorios remotos. Puede lograr la granularidad mediante la función SmartControl en Citrix Gateway.

Sin embargo, la situación cambia cuando la aplicación Citrix Workspace y Citrix Gateway pertenecen a cuentas empresariales distintas. En tales casos, el dominio del cliente no puede aplicar la función SmartControl porque la puerta de enlace no existe en el dominio. En su lugar, puede utilizar el proxy ICA saliente. La función proxy ICA saliente permite utilizar la función SmartControl incluso cuando la aplicación Citrix Workspace y Citrix Gateway se implementan en organizaciones distintas.

La aplicación Citrix Workspace admite inicios de sesión mediante el proxy de LAN de NetScaler. Utilice el plug-in de proxy saliente para configurar un único proxy estático o seleccione un servidor proxy en tiempo de ejecución.

Puede configurar proxies salientes a través de los métodos siguientes:

- Proxy estático: El servidor proxy se configura al proporcionarle un nombre de host y un número de puerto.
- Proxy dinámico: Se puede seleccionar un servidor proxy único entre uno o más servidores proxy mediante la DLL del plug-in de proxy.

Puede configurar el proxy saliente mediante la plantilla administrativa de objetos de directiva de grupo o el Editor del Registro.

Para obtener más información acerca del proxy saliente, consulte Compatibilidad con proxies ICA salientes en la documentación de Citrix Gateway.

#### Compatibilidad con proxies salientes: Configuración

> **Nota:**
>
> Si se configuran tanto proxies estáticos como proxies dinámicos, la configuración de proxies

> dinámicos tiene prioridad.

**Configurar el proxy saliente mediante la plantilla administrativa de GPO:**

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Citrix Workspace** > **Redirección de red**.
3. Seleccione una de estas opciones:
   - Para proxies estáticos: Seleccione la directiva **Configurar el proxy de LAN de NetScaler manualmente**. Seleccione **Habilitado** y, a continuación, indique el nombre de host y el número de puerto.
   - Para proxies dinámicos: Seleccione la directiva **Configurar el proxy de LAN de NetScaler con DLL**. Seleccione **Habilitado** y, a continuación, indique la ruta de acceso completa al archivo DLL. Por ejemplo: `C:\Workspace\Proxy\ProxyChooser.dll`.
4. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**

**Configurar el proxy saliente mediante el Editor del Registro:**

- **Para proxies estáticos:**
  - Abra el Editor del Registro y vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler`.
  - Cree claves de valor DWORD de la siguiente manera:

    ```
    "StaticProxyEnabled"=dword:00000001
    "ProxyHost"="testproxy1.testdomain.com
    "ProxyPort"=dword:000001bb
    ```

- **Para proxies dinámicos:**
  - Abra el Editor del Registro y vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler LAN Proxy`.
  - Cree claves de valor DWORD de la siguiente manera:

    ```
    "DynamicProxyEnabled"=dword:00000001
    "ProxyChooserDLL"="c:\\Workspace\\Proxy\\ProxyChooser.dll"
    ```

## Conexiones y certificados

### Conexiones

- Almacén HTTP
- Almacén HTTPS
- Citrix Gateway 10.5 y versiones posteriores

**Certificados**

> **Nota:**
>
> La aplicación Citrix Workspace para Windows está firmada digitalmente. La firma digital contiene una marca de tiempo. Por lo tanto, el certificado es válido incluso después de haber caducado.

- Privados (autofirmados)
- Raíz
- Carácter comodín
- Intermedios

**Certificados privados (autofirmados)**

Si existe un certificado privado en la puerta de enlace remota, instale el certificado raíz de la entidad de certificación de la organización en el dispositivo de usuario que accede a los recursos de Citrix.

> **Nota:**
>
> Si el certificado de la puerta de enlace remota no se puede verificar durante la conexión, aparece una advertencia de certificado que no es de confianza. Esta advertencia aparece cuando falta el certificado raíz en el almacén de claves local. Cuando un usuario elige ignorar la advertencia y continuar con la conexión, se muestran las aplicaciones, pero no se pueden iniciar.

**Certificados raíz**

Para equipos unidos a dominios, puede utilizar una plantilla administrativa de objeto de directiva de grupo para distribuir y configurar la confianza en los certificados de la CA.

Para equipos que no están unidos a un dominio, la organización puede crear un paquete de instalación personalizado para distribuir e instalar el certificado de la CA. Póngase en contacto con el administrador del sistema para recibir ayuda.

**Certificados comodín**

Se usan certificados comodín en un servidor dentro del mismo dominio.

La aplicación Citrix Workspace admite certificados comodín. Use certificados comodín de acuerdo con la directiva de seguridad de su organización. Una alternativa a los certificados comodín es un certificado que contenga la lista de nombres de servidor con la extensión del nombre alternativo del sujeto (SAN). Las entidades de certificación privadas o públicas emiten esos certificados.

#### Certificados intermedios

Si la cadena de certificados incluye un certificado intermedio, deberá agregar este certificado al certificado del servidor de Citrix Gateway. Para obtener información, consulte Configurar certificados intermedios.

#### Lista de revocación de certificados

La lista de revocación de certificados (CRL) permite a la aplicación Citrix Workspace comprobar si el certificado del servidor está revocado. La comprobación del certificado mejora la autenticación criptográfica del servidor y la seguridad general de la conexión TLS entre el dispositivo de usuario y un servidor.

La comprobación de la revocación de certificados (CRL) se puede habilitar en varios niveles. Por ejemplo, es posible configurar la aplicación Citrix Workspace para que verifique solo la lista local de certificados, o para que verifique las listas de certificados locales y de red. También puede configurar la verificación de certificados para permitir que los usuarios inicien sesiones solo cuando se verifiquen todas las listas de revocación de certificados.

Si quiere configurar la comprobación de certificados en su equipo local, cierre la aplicación Citrix Workspace. Compruebe que todos los componentes de Citrix Workspace, incluida la **Central de conexiones**, estén cerrados.

Para obtener más información, consulte Transport Layer Security.

### Función para mitigar los ataques de tipo “Man in the middle”

La aplicación Citrix Workspace para Windows le ayuda a reducir el riesgo de ataques de tipo “Man in the middle” mediante la función **Asingación de certificados de empresa** de Microsoft Windows. Un ataque de tipo “Man in the middle” es un tipo de ciberataque en el que el atacante intercepta y retransmite mensajes en secreto entre dos partes que creen que se están comunicando directamente entre sí.

Antes, al contactar con el servidor del almacén, no había forma de comprobar si la respuesta recibida provenía del servidor con el que intentaba contactar. Con la función **Asignación de certificados de empresa** de Microsoft Windows, puede comprobar la validez y la integridad del servidor mediante la asignación de su certificado.

La aplicación Citrix Workspace para Windows está preconfigurada para saber qué certificado de servidor debe esperar para un dominio o sitio en particular mediante las reglas de asignación de certificados. Si el certificado del servidor no coincide con el certificado de servidor preconfigurado, la aplicación Citrix Workspace para Windows bloquea la sesión.

Para obtener información sobre cómo implementar la función **Asignación de certificados de empresa**, consulte la documentación de Microsoft.

> **Nota:**
>
> Debe conocer la caducidad del certificado y actualizar correctamente las directivas de grupo y las listas de certificados de confianza. De lo contrario, es posible que no pueda iniciar la sesión aunque no haya ningún ataque.

## Storebrowse

April 6, 2023

> **Nota:**
>
> Este artículo solo se aplica a las implementaciones locales de Citrix Workspace. Para las implementaciones de la nube, consulte la documentación de Storebrowse para Workspace.

**Storebrowse** es una utilidad de línea de comandos que interactúa entre el cliente y el servidor. Se usa para autenticar todas las operaciones en StoreFront y con Citrix Gateway.

Con la utilidad **Storebrowse**, los administradores pueden automatizar las siguientes operaciones:

- Agregar un almacén.
- Producir una lista de las aplicaciones y los escritorios publicados desde un almacén configurado.
- Generar un archivo ICA manualmente seleccionando cualquier escritorio o aplicación virtual publicados.
- Generar un archivo ICA mediante la línea de comandos de **Storebrowse**.
- Iniciar la aplicación publicada.

La utilidad **Storebrowse** forma parte del componente `Authmanager`. Al completar la instalación de la aplicación Citrix Workspace, la utilidad **Storebrowse** se encuentra en la carpeta de instalación `AuthManager`.

Puede verificar si la utilidad **Storebrowse** está instalada junto con el componente `Authmanager`. Para ello, consulte la siguiente ruta de registro:

**Cuando los administradores instalan la aplicación Citrix Workspace:**

| | |
|---|---|
| En una máquina de 32 bits | [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManager\Inst |
| En una máquina de 64 bits | [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\A |

**Cuando los usuarios (no los administradores) instalan la aplicación Citrix Workspace:**

| | |
|---|---|
| En una máquina de 32 bits | [HKEY_CURRENT_USER\SOFTWARE\Citrix\AuthManager\Insta |
| En una máquina de 64 bits | [HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Citrix\Au |

## Requisitos

- Aplicación Citrix Workspace 1808 para Windows o una versión posterior.
- Mínimo 530 MB de espacio libre en disco.
- 2 GB de RAM.

### Tabla de compatibilidad

La utilidad **Storebrowse** es compatible con estos sistemas operativos:

| Sistema operativo |
|---|
| Windows 10 (ediciones de 32 y 64 bits) |
| Windows Server 2022 |
| Windows Server 2016 |
| Windows Server 2008 R2, edición de 64 bits |
| Windows Server 2008 R2, edición de 64 bits |

### Conexiones

La utilidad **Storebrowse** admite estos tipos de conexiones:

- Almacén HTTP
- Almacén HTTPS
- Citrix Gateway 11.0 y versiones posteriores

> **Nota:**
>
> En un almacén HTTP, la utilidad **Storebrowse** no acepta credenciales introducidas desde la línea de comandos.

#### Métodos de autenticación

##### Servidores de StoreFront

StoreFront admite diferentes métodos de autenticación para acceder a los almacenes; sin embargo, no todos se recomiendan. Por motivos de seguridad, algunos de los métodos de autenticación están inhabilitados de forma predeterminada cuando se crea un almacén.

- **Nombre de usuario y contraseña**: Introduzca las credenciales para autenticarse y acceder a los almacenes. La autenticación explícita está habilitada de forma predeterminada cuando crea el primer almacén.
- **PassThrough de dominio**: Después de autenticarse en los equipos Windows unidos a un dominio, se inicia sesión automáticamente en los almacenes. Para utilizar esta opción, habilite la autenticación PassThrough al instalar la aplicación Citrix Workspace. Para obtener más información sobre PassThrough de dominios, consulte Configurar la autenticación PassThrough.
- **HTTP básica**: Este método lo utilizan portales web e integraciones de clientes de terceros, donde se usa una interfaz de usuario externa para capturar un nombre de usuario y una contraseña aptos para el dominio. StoreFront utiliza la función de autenticación básica de IIS para transportar las credenciales al servidor de StoreFront. A continuación, StoreFront utiliza los Servicios de dominio o la autenticación de XML Broker Service para validar las credenciales y obtener la información del grupo. Para obtener información sobre cómo habilitar la autenticación HTTP básica, consulte HTTP básica en la documentación sobre Administrar métodos de autenticación.

La utilidad **Storebrowse** permite la autenticación de cualquiera de estas maneras:

- Mediante el componente `AuthManager`, integrado en la utilidad **Storebrowse**. Nota: Habilite el método de autenticación HTTP básica en StoreFront mientras trabaje con la utilidad **Storebrowse**. Este método es aplicable cuando el usuario proporciona las credenciales mediante los comandos de **Storebrowse**.
- Utilice el `Authmanager` que se incluye en la aplicación Citrix Workspace para Windows. Puede utilizar este método cuando utilice la autenticación Pass-Through de dominio. Para obtener más información, consulte la documentación de Autenticación PassThrough de dominio.

### Iniciar una aplicación o un escritorio publicado

Ahora puede iniciar un recurso directamente desde el almacén, sin tener que usar ningún archivo ICA.

### Uso de comandos

En la siguiente sección se ofrece información detallada sobre los comandos que se pueden usar desde la utilidad **Storebrowse**.

**Agregar un almacén**

`-a, --addstore`

**Descripción:**

Agrega un nuevo almacén. Devuelve la dirección URL completa del almacén. Si la devolución falla, se notifica un error.

> **Nota:**
>
> Con la utilidad **Storebrowse**, es posible configurar varios almacenes.

**Ejemplo de comando en StoreFront:**

Comando:

```
storebrowse.exe -U *username* -P *password* -D *domain* -a *URL of Storefront
*
```

Ejemplo:

'.\storebrowse.exe –U {nombre de usuario} –P {contraseña} –D {dominio} –a https://mi.primeralmacéndeejemplo.n

**Ejemplo de comando en Citrix Gateway:**

Comando:

```
storebrowse.exe -U *username* -P *password* -D *domain* -a *URL of CitrixGateway
*
```

Ejemplo:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -a <https://
mysecondexample.com>
```

**Ayuda**

`/?`

**Descripción:**

Ofrece información detallada sobre el uso de la utilidad **Storebrowse**.

**Enumerar almacenes**

`(-l),--liststore`

**Descripción:**

Ofrece una lista de los almacenes que agrega el usuario.

**Ejemplo de comando en StoreFront:**

```
.\storebrowse.exe -l
```

**Ejemplo de comando en Citrix Gateway:**

```
.\storebrowse.exe -l
```

#### Enumerar

```
(-M 0x2000 -E)
```

**Descripción:**

Enumera recursos.

Ejemplo de comando en StoreFront:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0x2000 -E
<https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Ejemplo de comando en Citrix Gateway:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0x2000 -E
<https://my.secondexample.net>
```

#### Inicio rápido

`-q`, `--quicklaunch`

**Descripción:**

Genera el archivo ICA para las aplicaciones y los escritorios publicados mediante la utilidad **Storebrowse**. La opción `quicklaunch` requiere una URL de inicio como entrada, junto con la URL del almacén. La URL de inicio puede ser el servidor de StoreFront o la URL de Citrix Gateway. El archivo ICA se genera en el directorio `%LocalAppData%\Citrix\Storebrowse\cache`.

Puede obtener la URL de inicio para cualquier aplicación y escritorio publicados si ejecuta el siguiente comando:

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/
discovery
```

Las URL de inicio suelen ser así:

```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix/
Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

Ejemplo de comando en StoreFront:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -q { Launch_URL_of_publ
 apps and desktops } <https://my.firstexamplestore.net/Citrix/Store/resources
/v2/Q2hJkOlmNoPQrSTV9y/launch/ica> <https://my.firstexamplestore.net/Citrix
/Store/discovery>
```

Ejemplo de comando en Citrix Gateway:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -q { Launch_URL_of_publ
 apps and desktops } <https://my.secondexmaplestore.com>
```

#### Inicio

`-L, --launch`

**Descripción:**

Genera el archivo ICA requerido para las aplicaciones y los escritorios publicados mediante la utilidad **Storebrowse**. La opción de inicio requiere el nombre del recurso y la URL del almacén. El nombre puede ser el servidor de StoreFront o la URL de Citrix Gateway. El archivo ICA se genera en el directorio `%LocalAppData%\Citrix\Storebrowse\cache`.

Ejecute este comando para obtener el nombre simplificado de las aplicaciones y los escritorios publicados:

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/
discovery
```

Este comando da como resultado lo siguiente:

```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix/
Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

El nombre en negrita del resultado anterior se usa como parámetro de entrada para la opción de inicio.

Ejemplo de comando en StoreFront:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -L  "{
Resource_Name } <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Ejemplo de comando en Citrix Gateway:

```
<.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -L { Resource_Name
 } https://my.secondexamplestore.com>
```

#### Lanzamiento de sesiones

`-S, --sessionlaunch`

**Descripción:**

Con este comando, puede agregar un almacén y verificar e iniciar los recursos publicados. Esta opción toma los siguientes elementos como parámetros:

- Nombre de usuario
- Contraseña
- Dominio
- Nombre del recurso que se va a iniciar
- URL del almacén

Sin embargo, si el usuario no proporciona las credenciales, `AuthManager` le pide que introduzca las credenciales y, a continuación, se inicia el recurso.

Puede obtener el nombre del recurso de aplicaciones y escritorios publicados con este comando:

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/
discovery
```

Este comando da como resultado lo siguiente:

```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix/
Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

El nombre en negrita del resultado anterior se usa como el parámetro de entrada de la opción `-S`.

Ejemplo de comando en StoreFront:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -S "{
Friendly_Resource_Name } <https://my.firstexamplestore.net/Citrix/Store/
discovery >
```

Ejemplo de comando en Citrix Gateway:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -S { Friendly_Resource_
 } <https://my.secondexamplestore.com>
```

**Carpeta de archivos**

`-f`, `--filefolder`

**Descripción:**

Genera el archivo ICA en la ruta personalizada para las aplicaciones y escritorios publicados.

La opción de inicio requiere un nombre de carpeta y el nombre del recurso como entrada con la URL del almacén. La URL del almacén puede ser el servidor de StoreFront o la URL de Citrix Gateway.

Ejemplo de comando en StoreFront:

```
.\storebrowse.exe -f "C:\Temp\Launch.ica" -L "Resource_Name" { Store }
```

Ejemplo de comando en el dispositivo Citrix Gateway:

```
.\storebrowse.exe -f "C:\Temp\Launch.ica" -L "Resource_Name" { NSG_URL }
```

#### Autenticación del seguimiento

`-t, --traceauthentication`

**Descripción:**

Genera registros para el componente `AuthManager`. Los registros se generan solo si la utilidad **Storebrowse** utiliza un `AuthManager` integrado. Los registros se generan en el directorio `localappdata%\Citrix\Storebrowse\logs`.

> **Nota:**
>
> Esta opción no puede ser el último parámetro que aparece en la línea de comandos del usuario.

Ejemplo de comando en StoreFront:

```
.\storebrowse.exe -t -U { UserName } -P { Password } -D { Domain } -a { StoreURL }
```

Ejemplo de comando en Citrix Gateway:

```
.\storebrowse.exe -t -U { UserName } -P { Password } -D { Domain } -a { NSG_URL }
```

#### Eliminar un almacén

`-d, --deletestore`

**Descripción:**

Elimina el almacén StoreFront o Citrix Gateway existente.

Ejemplo de comando en StoreFront:

```
.\storebrowse.exe -d https://my.firstexamplestore.net/Citrix/Store/discovery
```

Ejemplo de comando en Citrix Gateway:

```
.\storebrowse.exe -d https://my.secondexmaplestore.com
```

### Función Single Sign-On en Citrix Gateway

Single Sign-On permite autenticarse en un dominio y usar Citrix Virtual Apps and Desktops y Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) que proporciona el dominio. Puede iniciar sesión sin tener que reautenticarse en cada aplicación o escritorio. Al agregar un almacén, las credenciales se transfieren al servidor de Citrix Gateway, junto con las aplicaciones y los escritorios de Citrix Virtual Apps and Desktops y Citrix DaaS, y los parámetros del menú Inicio.

Esta función es compatible con Citrix Gateway versión 11 y posteriores.

**Requisitos previos:**

Si quiere ver los requisitos previos necesarios para configurar el inicio Single Sign-On en Citrix Gateway, consulte Configurar la autenticación PassThrough de dominio.

La función Single Sign-On con Citrix Gateway puede habilitarse mediante la plantilla administrativa de objeto de directiva de grupo (GPO).

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas** > **Componentes de Citrix** > **Citrix Workspace** > **Autenticación de usuarios** > **Single Sign-On para Citrix Gateway**.
3. Utilice las opciones de activación o desactivación para habilitar o inhabilitar la opción Single Sign-On.
4. Haga clic en **Aplicar** y, a continuación, en **Aceptar.**
5. Reinicie la sesión de la aplicación Citrix Workspace para que los cambios surtan efecto.

**Limitaciones:**

- El método de **autenticación HTTP básica** debe estar habilitado en el servidor de StoreFront para las operaciones de introducción de credenciales con la utilidad **Storebrowse**.
- Si tiene un almacén HTTP e intenta conectarse al almacén mediante la utilidad para comprobar o iniciar las aplicaciones o escritorios virtuales publicados, no se permite introducir credenciales mediante la opción de línea de comandos. Como solución temporal, utilice el módulo `AuthManager` externo si no proporciona credenciales mediante la línea de comandos.
- Actualmente, la utilidad **Storebrowse** solo admite Citrix Gateway configurado en un único almacén en el servidor de StoreFront.
- La introducción de credenciales en la utilidad **Storebrowse** solo funciona si Citrix Gateway está configurado con el método de autenticación con factor único.
- Las opciones de línea de comandos `Username (-U)`, `Password (-P)` y `Domain (-D)` de la utilidad **Storebrowse** distinguen entre mayúsculas y minúsculas, y deben contener solo mayúsculas.

Para habilitar SSON para aplicaciones de terceros que usan ICOSDK, cree este Registro:

- Clave del Registro: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\NonIEAppsWithSson`
- Valor del Registro: Ruta completa de las aplicaciones de terceros
- Tipo de Registro: reg_multi_sz

Ejemplo:

- Clave del Registro: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\NonIEAppsWithSson`

- Valor del Registro: C:\temp1\abc.exe; C:\temp2\xyz.exe
- Tipo de Registro: reg_multi_sz

> **Nota:**
>
> - Puede proporcionar varias aplicaciones de terceros separadas por puntos y comas.
> - Esta función es compatible a partir de la versión 2107.

## Storebrowse para Workspace

April 6, 2023

La aplicación Citrix Workspace para Windows permite usar **Storebrowse** en la implementación local y de autoservicio de la aplicación Citrix Workspace. También permite a los usuarios de **Storebrowse** acceder a las funciones de Cloud y Workspace.

> **Nota:**
>
> - Este artículo solo se aplica a las implementaciones de la nube de Citrix Workspace. Para las implementaciones locales, consulte la documentación de Storebrowse.
> - Esta función permite usar **Storebrowse** solamente con Single Sign-On.
> - Los requisitos previos mencionados en Requisitos y compatibilidad del sistema deben estar disponibles para usar esta función.

### Uso de comandos

En la siguiente sección se ofrece información detallada sobre los comandos que se pueden usar desde la utilidad **Storebrowse**.

> **Nota:**
>
> - Esta función también admite otros comandos del plug-in de autoservicio, como se menciona en CTX200337.
> - Puede ejecutar estos comandos en el símbolo del sistema.

- `-a "discoveryurl"`: Agrega un almacén a través de la línea de comandos. Este comando no muestra el mensaje de autenticación cuando SSO está habilitado. Por ejemplo, los dominios de AAD se unen a dispositivos donde la autenticación se realiza a través de la vista web. En los demás dispositivos, aparece el mensaje de autenticación.
  - Ejemplo:`SelfService.exe storebrowse -a "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`
- `-d "discoveryurl"`: Elimina el almacén.

  - Ejemplo:`SelfService.exe storebrowse -d "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`

- `-e "discoveryurl"`: Exporta los detalles del recurso en formato JSON. Este comando almacena el archivo resource.json en la ubicación predeterminada `%LOCALAPPDATA%\citrix\selfservice`. La aplicación Citrix Workspace debe estar activa para ejecutar este comando y el usuario debe haber iniciado sesión.

  - Ejemplo:`SelfService.exe storebrowse -e "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`

  También puede especificar su propia ruta si no quiere almacenar el archivo resource.json en la ubicación predeterminada.

  - Ejemplo: `.\SelfService.exe storebrowse -e "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery""C:\Users\<username>\Documents\Fiddler2"`. Esto almacena el archivo resource.json en `C:\Users\<username>\Documents\Fiddler2`.

- `-q "FriendlyName""discoveryurl"`: Utilice este comando para ejecutar rápidamente el recurso especificado.

  - Ejemplo:`SelfService.exe storebrowse -q "Excel 2016""https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`

- `-launch "launchcommandline"`: Inicio de recursos mediante “launchcommandline” desde resource.json.

  > **Nota:**
  >
  > - Copie la línea “launchcommandline” de resource.json.
  > - Quite **/** de la línea “launchcommandline” especificada en el archivo resource.json antes de ejecutar el comando.

  - Ejemplo:`SelfService.exe storebrowse -launch -s store0-5c3ec017 -CitrixID store0-5c3ec017@@a9a8e3ac-099d-4577-b84e-e33d0695df39. Notepad -ica "https://cwawiniwstest.cloudburrito.com/Citrix/Store/resources/v2/YTlhOGUzYWMtMDk5ZC00NTc3LWI4NGUtZTMzZDA2OTVkZjM5Lk5vdGVwYWQ-/launch/ica"-cmdline`

  Después de ejecutar `-launch "launchcommandline"`, el archivo ICA se almacenará en el directorio `%LOCALAPPDATA%\citrix\selfservice\cache`. Haga doble clic en el archivo ICA para iniciar el recurso.

- `-liststore`: Enumera los almacenes que se agregan dentro de SSP. Es una lista de almacenes que incluye storeID y la URL de detección de cada almacén.

  - Ejemplo:`SelfService.exe storebrowse -liststore`

> **Nota:**
>
> La aplicación Citrix Workspace debe estar activa para ejecutar el comando `-liststore`.

El comando `Selfservice.exe storebrowse -liststore` almacena el archivo storedetails.json en `AppData\Local\Citrix\SelfService`.

## Desktop Lock de la aplicación Citrix Workspace

January 18, 2023

Puede usar Desktop Lock de la aplicación Citrix Workspace cuando no necesite interactuar con el escritorio local. Puede seguir usando Desktop Viewer (si está habilitado), pero solo verá el siguiente conjunto de opciones en la barra de herramientas:

- Ctrl+Alt+Supr
- Preferencias
- Dispositivos
- Desconectar.

La aplicación Citrix Workspace para Windows con Desktop Lock funciona en máquinas unidas a dominios con Single Sign-On habilitado y configuradas con un almacén. No admite sitios de PNA. Las versiones anteriores de Desktop Lock no se admiten después de actualizar a Citrix Receiver para Windows 4.2 o una versión posterior.

Instale la aplicación Citrix Workspace para Windows con el indicador `/includeSSON`. Configure el almacén y Single Sign-On, ya sea mediante el archivo adm/admx o con la opción de la línea de comandos. Para obtener más información, consulte Instalación.

A continuación, instale Desktop Lock de la aplicación Citrix Workspace como administrador con el archivo `CitrixWorkspaceDesktopLock.msi` disponible en la página de descargas de Citrix.

### Requisitos del sistema

- Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package. Para obtener más información, consulte la página de descargas de Microsoft.
- Compatible con Windows 10 (actualización Anniversary Update incluida) y Windows 11.
- Se conecta a StoreFront solo a través de protocolos nativos.
- Puntos finales unidos a un dominio.
- Los dispositivos de usuario deben estar conectados a una LAN o una WAN.

### Acceso a aplicaciones locales

> **Importante**
>
> Al habilitar el acceso a aplicaciones locales, se puede permitir el acceso al escritorio local, a menos que se haya aplicado un bloqueo completo mediante una plantilla de objeto de directiva de grupo o una directiva similar. Para obtener más información, consulte la sección Configurar el acceso a aplicaciones locales y la redirección de URL en la documentación de Citrix Virtual Apps and Desktops.

### Funcionamiento de Desktop Lock en la aplicación Citrix Workspace

- Puede usar Desktop Lock de la aplicación Citrix Workspace con las siguientes funcionalidades de la aplicación Citrix Workspace:
  - 3Dpro, Flash, USB, HDX Insight, plug-in de Microsoft Lync 2013 y acceso a aplicaciones locales
  - Solo autenticación de dos factores o autenticación con tarjeta inteligente
- Al desconectar la sesión de Desktop Lock de la aplicación Citrix Workspace, se cierra la sesión del dispositivo final.
- La redirección de Flash está inhabilitada en Windows 8 y versiones posteriores. La redirección de Flash está habilitada en Windows 7.
- Desktop Viewer está optimizado para Desktop Lock de la aplicación Citrix Workspace y no incluye las propiedades Inicio, Restaurar, Maximizar ni Pantalla.
- Ctrl+Alt+Supr está disponible en la barra de herramientas de Desktop Viewer.
- La mayoría de las teclas de acceso directo de Windows se pasan a la sesión remota, excepto Windows+L.
- Ctrl+F1 activa Ctrl+Alt+Supr cuando se inhabilita la conexión o Desktop Viewer para conexiones de escritorio.
- Se crea un perfil de usuario local en el dispositivo final cuando el usuario inicia sesión en el sistema. El perfil se conserva en el dispositivo final incluso cuando el usuario cierra sesión y se basa en las configuraciones de la administración de perfiles.

> **Nota:**
>
> Con Desktop Lock instalado y `LiveInDesktopDisconnectOnLock` establecido en **False** en la ruta del Registro `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle` o en `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle`, la sesión activa se desconecta cuando el dispositivo de punto final sale de la hibernación o del modo de espera.

### Instalar Desktop Lock de la aplicación Citrix Workspace

Con este procedimiento, se instala la aplicación Citrix Workspace para Windows de forma que los escritorios virtuales aparezcan mediante Desktop Lock de la aplicación Citrix Workspace. En el caso de

implementaciones que utilizan tarjetas inteligentes, consulte Tarjeta inteligente.

1. Inicie sesión con una cuenta de administrador local.
2. En el símbolo del sistema, ejecute este comando:

   Por ejemplo:

   ```
   CitrixWorkspaceApp.exe
        /includeSSON
   STORE0="DesktopStore;https://my.storefront.server/Citrix/MyStore/
      discovery;on;Desktop Store"
   <!--NeedCopy-->
   ```

   El comando está disponible en la aplicación Citrix Workspace y en la carpeta **Plug-ins** > **Windows** > **Citrix Workspace app** de los medios de instalación. Para obtener información detallada sobre los comandos, consulte la documentación sobre la instalación de la aplicación Citrix Workspace en Instalación.
3. En la misma carpeta de los medios de instalación, haga doble clic en `CitrixWorkspaceDesktopLock.msi`. Aparece el asistente de Desktop Lock. Siga las indicaciones.
4. Cuando se complete la instalación, reinicie el dispositivo de usuario. Si dispone de permisos para acceder a un escritorio e inicia sesión como un usuario de dominio, el dispositivo se muestra mediante Desktop Lock de la aplicación Citrix Workspace.

Puede permitir la administración del dispositivo de usuario una vez finalizada la instalación. La cuenta que se utilizó para instalar `CitrixWorkspaceDesktopLock.msi` se excluye del shell de sustitución. Si esa cuenta se elimina más tarde, no puede iniciar sesión ni administrar el dispositivo.

Para ejecutar una **instalación silenciosa** de Citrix Workspace Desktop Lock, use la siguiente línea de comandos:

```
msiexec /i CitrixWorkspaceDesktopLock.msi /qn
```

### Configurar Desktop Lock de la aplicación Citrix Workspace

Una vez que haya iniciado sesión como un usuario que no es administrador, Desktop Lock inicia automáticamente una sesión de escritorio asignada.

Mediante directivas de Active Directory, impida que los usuarios pongan a hibernar los escritorios virtuales.

Para configurar Desktop Lock de la aplicación Citrix Workspace, use la misma cuenta de administrador que utilizó para instalarlo.

- Compruebe si los archivos receiver.admx (o receiver.adml) y receiver_usb.admx (.adml) se han cargado en las Directivas de grupo (las directivas aparecen en Configuración del equipo o en **Configuración de usuario** > **Plantillas administrativas** > **Plantillas administrativas clásicas (ADMX)** > **Componentes de Citrix**). Los archivos ADMX están en %ProgramFiles%\Citrix\ICA Client\Configuration\.
- Preferencias de USB. Cuando un usuario conecta un dispositivo USB, ese dispositivo se comunica automáticamente de forma remota con el escritorio virtual y no se requiere ninguna interacción por parte del usuario. El escritorio virtual controla el dispositivo USB y lo muestra en la interfaz de usuario.
  - Habilite la regla de directivas USB.
  - En **Aplicación Citrix Workspace** > **Uso remoto de dispositivos cliente** > **Uso remoto de USB genérico**, habilite y configure las directivas Dispositivos USB existentes y Dispositivos USB nuevos.
- Asignación de unidades: En **Aplicación Citrix Workspace** > **Uso remoto de dispositivos cliente**, habilite y configure la directiva Asignación de unidades del cliente.
- Micrófono: En **Aplicación Citrix Workspace** > **Uso remoto de dispositivos cliente**, habilite y configure la directiva Micrófono del cliente.

### Configurar tarjetas inteligentes para su uso con Desktop Lock para Windows

1. Configure StoreFront.
   a) Configure XML Service para usar resolución de direcciones DNS para poder usar Kerberos.
   b) Configure los sitios de StoreFront para el acceso mediante HTTPS, cree un certificado de servidor firmado por la entidad de certificación de su dominio y agregue un enlace HTTPS al sitio web predeterminado.
   c) Compruebe que está habilitada la autenticación PassThrough con tarjeta inteligente (está habilitada de manera predeterminada).
   d) Habilite Kerberos.
   e) Habilite Kerberos y la autenticación PassThrough con tarjeta inteligente.
   f) Habilite el Acceso anónimo en el sitio web predeterminado de IIS y use la Autenticación de Windows integrada.
   g) Asegúrese de que el sitio web predeterminado de IIS no requiera SSL e ignore los certificados de cliente.
2. Use la Consola de administración de directivas de grupo para configurar las directivas de equipo local en el dispositivo de usuario.
   a) Importe la plantilla Receiver.admx desde %ProgramFiles%\Citrix\ICA Client\Configuration\.
   b) Expanda **Plantillas administrativas** > **Plantillas administrativas clásicas (ADMX)** > **Componentes de Citrix** > **Citrix Workspace** > **Autenticación de usuarios**.
   c) Habilite Autenticación con tarjeta inteligente.
   d) Habilite Nombre de usuario y contraseña locales.

3. Configure el dispositivo del usuario antes de instalar Desktop Lock de la aplicación Citrix Workspace.
    a) Agregue la dirección URL de Delivery Controller en la lista de Sitios de confianza de Internet Explorer en Windows.
    b) Agregue la URL del primer grupo de entrega a la lista de sitios de confianza de Internet Explorer. Agregue la URL en formato escritorio://nombre-grupo-de-entrega.
    c) Permita a Internet Explorer que utilice el inicio de sesión automático en caso de sitios de confianza.

Cuando Desktop Lock de la aplicación Citrix Workspace se instala en el dispositivo de usuario, se aplica una directiva de extracción de tarjetas inteligentes coherente. Por ejemplo, si la directiva de extracción de tarjetas inteligentes de Windows se establece en Forzar cierre de sesión para el escritorio, el usuario debe cerrar la sesión del dispositivo de usuario, independientemente de cuál sea la directiva de extracción de tarjeta inteligente configurada en el equipo. Desktop Lock garantiza que el dispositivo del usuario no quede en un estado incoherente. Esto se aplica solo a los dispositivos de usuario con Desktop Lock de la aplicación Citrix Workspace.

### Eliminar Desktop Lock

Asegúrese de quitar los dos componentes indicados a continuación:

1. Inicie sesión con la misma cuenta de administrador local que usó para instalar y configurar Desktop Lock de la aplicación Citrix Workspace.
2. Con la función de Windows para quitar o cambiar programas:
    - Quite Desktop Lock de la aplicación Citrix Workspace.
    - Quite la aplicación Citrix Workspace para Windows.

### Pasar teclas de acceso directo de Windows a la sesión remota

La mayoría de las teclas de acceso directo de Windows se pasan a la sesión remota. Esta sección describe algunas de las más comunes.

### Windows

- Win+D: Minimizar todas las ventanas en el escritorio.
- Alt+Tab: Cambiar la ventana activa.
- Ctrl+Alt+Supr: A través de Ctrl+F1 y la barra de herramientas de Desktop Viewer.
- Alt+Mayús+Tab
- Windows+Tab
- Windows+Mayús+Tab
- Windows+Todas las teclas de caracteres

### Windows 8

- Win+C: Abrir accesos.
- Win+Q: Acceso Buscar.
- Win+H: Acceso Compartir.
- Win+K: Acceso Dispositivos.
- Win+I: Acceso Configuración.
- Win+Q: Buscar en Aplicaciones.
- Win+W: Buscar en Configuración.
- Win+F: Buscar archivos.

### Aplicaciones de Windows 8

- Win+Z: Ir a opciones de la aplicación.
- Win+. : Acoplar aplicación a la izquierda.
- Win+Mayús+. : Acoplar aplicación a la derecha.
- Ctrl+Tab: Navegar en ciclo por el historial de aplicaciones.
- Alt+F4: Cerrar una aplicación.

### Escritorio

- Win+D: Abrir escritorio.
- Win+,: Vistazo de escritorio.
- Win+B: Volver al escritorio.

### Otros

- Win+U: Abrir el Centro de accesibilidad.
- Ctrl+Esc: Pantalla Inicio.
- Win+Entrar: Abrir el Narrador de Windows.
- Win+X: Abrir el menú de configuración de herramientas del sistema.
- Win+Impr Pant: Toma una captura de pantalla y la guarda en Imágenes.
- Win+Tab: Abre una lista de cambio de ventana.
- Win+T: Vista previa de ventanas abiertas en la barra de tareas.

## Kit de desarrollo de software (SDK) y API

February 17, 2023

### SDK de declaración de identidad de certificado

El SDK de declaración de identidad de certificado (CID) permite a los desarrolladores crear un plug-in. El plug-in permite que la aplicación Citrix Workspace se autentique en el servidor de StoreFront mediante el certificado que está instalado en la máquina cliente. CID declara la identidad de la tarjeta inteligente del usuario en un servidor de StoreFront sin realizar una autenticación basada en tarjeta inteligente.

La versión más reciente de la Declaración de identidad de certificado para Citrix Workspace para Windows es la versión **2212**.

Para obtener más información, consulte la documentación de CID SDK para la aplicación Citrix Workspace para Windows.

### Citrix Common Connection Manager SDK

Common Connection Manager (CCM) SDK proporciona un conjunto de API nativas que le permiten interactuar y realizar operaciones básicas de manera programática. Este SDK no requiere una descarga por separado porque forma parte del paquete de instalación de la aplicación Citrix Workspace para Windows.

> **Nota:**
>
> Algunas de las API que están relacionadas con el inicio de sesiones requieren que el archivo ICA comience el proceso de inicio de las sesiones de aplicaciones y escritorios virtuales.

Las capacidades del CCM SDK incluyen:

- Lanzamiento de sesiones
  - Permite iniciar aplicaciones y escritorios, mediante el archivo ICA generado.
- Desconexión de sesiones
  - Similar a la operación de desconexión mediante la Central de conexiones. La desconexión puede hacerse para todas las sesiones o para un usuario concreto.
- Cierre de sesiones
  - Similar a la operación de cierre de sesión mediante la Central de conexiones. Se pueden cerrar todas las sesiones o la sesión de un usuario concreto.
- Información de la sesión
  - Proporciona diferentes métodos para obtener información relacionada con la conexión de las sesiones iniciadas. La sesión incluye sesiones de escritorio, sesiones de aplicación y sesiones de aplicación integrada.

Para obtener más información acerca del SDK, consulte la guía Programmers guide to Citrix CCM SDK.

### Citrix Virtual Channel SDK

El kit de desarrollo de software (SDK) de Citrix Virtual Channel permite la escritura de aplicaciones del lado del servidor y controladores del lado del cliente para más canales virtuales que usan el protocolo ICA. Las aplicaciones de canal virtual del lado del servidor se encuentran en servidores Citrix Virtual Apps and Desktops. Si quiere escribir controladores virtuales para otras plataformas cliente, póngase en contacto con el equipo de Asistencia técnica de Citrix.

El Virtual Channel SDK ofrece:

- La API para Citrix Virtual Driver (VDAPI) se usa con las funciones de canal virtual en el SDK de WFAPI (Citrix Server API SDK) para crear nuevos canales virtuales. La función de canales virtuales proporcionada por VDAPI está diseñada para simplificar la creación de sus propios canales virtuales.
- La API de Windows Monitoring, que mejora la experiencia visual y la compatibilidad con aplicaciones de terceros integradas con ICA.
- Código fuente operacional de ejemplos de programas de canales virtuales, que demuestran varias técnicas de programación.
- El Virtual Channel SDK requiere el SDK de WFAPI para escribir la parte del lado del servidor del canal virtual.

La versión más reciente de Virtual Channel SDK para Windows es la version **2302**.

Para obtener, consulte la documentación de Citrix Virtual Channel SDK para la aplicación Citrix Workspace para Windows.

### API Credential Insertion de Fast Connect 3

La API Credential Insertion de Fast Connect 3 ofrece una interfaz que proporciona credenciales de usuario a la función Single Sign-On (SSON). Esta función está disponible a partir de la versión 4.2 de la aplicación Citrix Workspace para Windows. Con esta API, los socios de Citrix pueden ofrecer productos de autenticación y SSO que usen StoreFront para iniciar sesiones de usuarios en aplicaciones o escritorios virtuales y luego desconectar a los usuarios de esas sesiones.

La versión más reciente de la API de Fast Connect para Citrix Workspace para Windows es la versión **2212**.

Para obtener más información, consulte la documentación Fast Connect 3 Credential Insertion API for Citrix Workspace app for Windows.

### Scripts para implementar Citrix Workspace para Windows

Estos son scripts de ejemplo para implementar y configurar la aplicación Citrix Workspace.

La versión más reciente de los scripts para implementar Citrix Workspace para Windows es la versión **2212**.

## Referencia para parámetros ICA

January 18, 2023

En el archivo de referencia para parámetros ICA se ofrecen listas de parámetros de Registro y parámetros de archivos ICA, lo que permite a los administradores personalizar el comportamiento de la aplicación Citrix Workspace. También puede usar la Referencia para parámetros ICA a fin de solucionar problemas relacionados con un comportamiento inesperado de la aplicación Citrix Workspace.

Referencia para parámetros ICA (descarga en PDF)